جامعة الشهيد حمه لخضر – الوادي
كلية الحقوق والعلوم السياسية
قسم الحقوق

الأمن السيبراني

مذكرة تخرج ضمن متطلبات نيل شهادة الماستر في الحقوق
تخصص: جريمة و أمن

من إعداد الطالب:
ـ الـــــدام محمـــد

تحت إشراف الأستـــاذ:
ـ خـــلـــف فـــــاروق

لجنة المناقشة:

الاسم واللقب	الجامعة	الصفة
خيرجة ميلود	جامعة الشهيد حمه لخضر – الوادي	رئيسا
خلـف فـاروق	جامعة الشهيد حمه لخضر – الوادي	مشرفا
جرمون محمد الطاهر	جامعة الشهيد حمه لخضر – الوادي	مناقشا

السنة الجامعية: 2023/2022

الإهـداء

الحمد لله الذي أنار لي درب العلم والمعرفة و أعانني على أداء هذا الواجب
ووفقني إلى إنجاز هذا العمل

و الصلاة و السلام على الحبيب المصطفى.

أهدي ثمرة جهدي هذا:

إلى من إشتاقت أنفسنا لهم و هم تحت التراب

روح الوالدين العزيزين، رحمكما الله

إلـى عائلتي الصغيرة زوجتي، و إبنتي.

إلـى إخوتي وأخواتي كل بإسمه.

إلـى زملائي في الدراسة

إلـى كل من ساهم في انجاز هذا البحث المتواضع

شكـــر وتقـــدير

أتقـــدم بجـــزيل الشكر والتقـــدير:

إلـى الله سبحانه وتعالى الذي أعطانا الصحة والقوة لإتمام هذا البحث.

إلـى أستـاذنا الفاضـل (خلف فاروق) على قبوله الإشراف على مذكرتنا الذي لم يبخل علينا بتوجيهاته و نصائحه القيمة التي كانت عونا لي في إتمام هذا البحث.

إلى السادة أعضاء اللجنة على قبولهم مناقشة هذه المذكرة.

إلى جميع أساتذتنا بجامعة الشهيد حمه لخضر الوادي.

وكل من كان سندا لنا وشجعنا للوصول إلى هذه المرحلة

لكم منا فائق التقدير والإحترام.

الطالب: الـــــــداوي محمـــد

مقدمـــة

مقـــدمـــة:

لقد شهد العالم في هذه المرحلة المعاصرة تحولات جذرية عميقة، وبصفة مستمرة، في مجالات المعلومات والإتصالات بفضل الثورة التكنولوجية التي غّيرت حياة المجتمعات بشكل جوهري. وهي مستمرة في إحداث التغّيرات في المجالات الأخرى، الثقافية والسياسية والاقتصادية والعلمية والاجتماعية.

وفي إطار الشبكة المعلوماتية والمعرفية المعقدة وإنتاجها أصبحت نواة التنظيم الاجتماعي تتمحور حول المعلومة بكل أنواعها، نظرا للإعتماد المتزايد على المعلومات العلمية والتكنلوجية وإستخدام تكنولوجيا المعلومات كالإتصالات في تطبيقات متنوعة.

ومن هنا ولدت جرائم جديدة إختلفت عن الجرائم التقليدية إتسمت بخطورتها الكبيرة نظرا لطابعها الخاص سواءاً ما يميز الجريمة أو مرتكبها وصعوبة الإثبات فيها، وقد تثار مشكلة الأمن السيبراني الذي يعد مهمة صعبة في ظل الجريمة الإلكترونية التي لا تعترف بالحدود و الأوطان ويعيش محترفوها في عالم إفتراضي ، فتطور الأمن السيبراني بات أمراً حتميا وهاجساً أمام رجال القانون ، فكان من الضرورة التصدي لبوادر هذه الجرائم كي لا تستفحل مع وتيرة النمو المتسارع الذي تشهده الدول ومن بينها الجزائر في إستخدام النظم المعلوماتية فضلا عن ظروف العولمة والتبعية التكنولوجية من مناخ موات لإنتهاك حرمة البيانات الشخصية والمساس بالأمن القومي لهذه الدول و سيادتها الوطنية. ومن هنا تتجلى أهمية موضوع " الأمن السيبراني والجرائم السيبرانية وآليات مكافحتها". وهذا ما سنحاول إماطة اللثام حوله في النقاط التالية:

أولا/ أهميـــة الموضـوع

تبرز أهمية الموضوع في حداثته ومدى مساسه بالواقع وإمتداد خطره، حيث لم يعد مقتصراً على خصوصية الأفراد، بل أنه إمتد إلى الدول ذاتها.

كما تجلت أهمية البحث في بيان طرق وأساليب الحماية المعلوماتية أو ما عرف بالأمن السيبراني، ودوره في قمع الجريمة.

وبالتالي يمكن الإستفادة من هذه الدراسة في مواجهة جرائم الأنترنت والتعامل معها ومكافحتها، ولفت إنتباه الأجهزة المختصة إلى سلوكيات وأفعال جنائية ترتكب ضد الآخرين بواسطة الحاسب الآلي ومن خلال شبكة الإنترنت، إذ لابد من مواجهتها بضوابط قانونية وقضائية وأمنية.

ثانيا / أهداف البحـث والدراسـة

تهدف الدراسة إلى تبيان مفهوم الأمن السيبراني وتحديد الجرائم السيبرانية التي تعتمد على تكنولوجيات المعلومات والإتصالات بمختلف تطبيقاتها الموجودة وكذا تحديد بعض المفاهيم المتعلّقة بالجرائم الإلكترونية بعد تشخيص واقعها ورصد أبعادها، مع معرفة كيفية تعامل الدول والجزائر معها وخاصة إبراز إهتمام المشّرع الجزائري ومدى توفيره الإطار القانوني والمواكب للمتغيرات المتسارعة للثورة الرقمية بهدف مواجهتها مع تأهيل الموارد البشرية المتخصصة وتكوينها في هذا المجال.

ثالثا / أسبـاب اختيار الموضـوع

كان لإختيارنا هذا الموضوع عدة أسباب منها:

1) أسباب ذاتية:

- ميولنا الشخصي لهذا الموضوع ورغبتنا بالبحث فيه.
- الرغبة في المساهمة ولو لجزء بسيط في إثراء المكتبة القانونية.

2) أسباب موضوعية:

التطلع لتبيان أهمية الأمن السيبراني ودوره في حياتنا اليومية التي أضحت لا تخلو من المعاملات الإلكترونية بمختلف أشكالها والتهديدات التي تحيط بها.

رابعا / إشكاليـــة الدراســة

أضحى العالم اليوم يتطلب زيادة كبيرة في الوعي وإدراك المخاطر كالتهديدات التي تفرضها إستعمال تكنولوجيات المعلومات كالإتصالات في الفضاء السيبراني مما يستدعي إهتماما أكبر بالحماية منها، مع تسطير إستراتيجية وطنية شاملة تستجيب للمتطلبات الوطنية والإقليمية والدولية من أجل ضمان أمن المعلومات في الفضاء السيبراني بإعتبارها الأساس لضمان الأمن الوطني بمفهومه الشامل.

ولكي نتمكن من إستيعاب الموضوع والتدقيق فيه جرى التركيز على البحث في الإشكالية التالية:

- ما هو دور الأمن السيبراني في مكافحة الجرائم الالكترونية؟

وقصد الإلمام بجوانب الموضوع المختلفة والمتشابكة نوعا، فّككنا الإشكالية إلى التساؤلات التالية:

1-ما مفهوم الأمن السيبراني؟

2-ماهي الجرائم السيبرانية؟

3-ما هي الجهود الدولية والإقليمية والوطنية المبذولة لمحاربة الجرائم السيبرانية؟

خامسا/ المنهجيــة المتبعــة في الدراســة

إعتمدنا في البحث على المنهج الوصفي والمنهج التحليلي وذلك للتعرف على الأمن السيبراني وكذا الجرائم السيبرانية وخصائصها وأنواعها، وتبيان مدى خطورتها على كافة فئات المجتمع وأمنهم الإجتماعي ليس على المستوى المحلي فقط بل يشمل المستوى الإقليمي والدولي.

فضلا عن إستعانتنا بالمنهج المقارن في الإشارة إلى قوانين وتشريعات دول عدة عانت من تنامي جرائم الإعتداء على الفضاء السيبراني.

سادسا/ الدراسات السابقة:

استندنا في البحث على العديد من الدراسات السابقة الحديثة الي تم إعدادها من طرف أساتذة و دكاترة في شكل مقالات علمية و قانونية تناولوا في مجملهم الإطار المفاهيمي للأمن السيبراني و الجريمة السيبرانية، و آليات مكافحة الجرائم السيبرانية على المستويين الدولي و الوطني، وقد تم إدراج هذه الدراسات كمصادر في قائمة المراجع، يمكن أن نذكر منها على سبيل المثال لا الحصر:

- الإستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، دراسة للدكتور جمال الدين دندن، وهي منشورة في مجلة صوت القانون، جامعة الجيلالي بو نعامة، خميس مليانة، المجلد 07، العدد 02، 2020، قدم فيها الباحث الآليات المؤسساتية المختلفة والمتخصصة في مكافحة الجرائم السيبرانية على المستوى الوطني.
- الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات، دراسة للدكتور بارة سمير ، منشورة في المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، المجلد 02، العدد 04، 2017، قدم فيها الباحث أساسيات عن الأمن السيبراني وأبعاده و كذا ماهية الجريمة السيبرانية و أنماط التهديدات السيبرانية، بالإضافة إلى الأجهزة الأمنية الجزائرية المختصة بمكافحة الجرائم السيبرانية، وفي الختام عدد الباحث عوائق تحقيق الأمن السيبراني في ظل التحديات الآنية و المستقبلية.

سابعا/ خطــة الدراســة

لغرض دراسة البحث والإلمام بالموضوع ارتأيت الخطة التالية:

في الفصل الأول خصصناه للأمن السيبراني والجرائم السيبرانية ويضم مبحثين:

الأول عنوانه نطاق و مجال الأمن السيبراني، والثاني يشمل الجرائم السيبرانية.

أما الفصل الثاني تناولنا فيه آليات مكافحة الجرائم السيبرانية ويحتوي على مبحثين:

الأول منه خصصناه لآليات مكافحة الجرائم السيبرانية على الصعيد الدولي، أما المبحث الثاني لآليات مكافحة الجرائم السيبرانية على الصعيد الوطني.

وفي نهاية دراستنا وضعنا خاتمة ضممناها مختلف النتائج والإقتراحات المستخلصة من الدراسة.

الفصل الأول:

الأمن السيبراني

و

الجريمة السيبراني

الفصل الأول:

الأمن السيبراني و الجريمة السيبرانية

أصبح عصرنا الحالي يتصف بعصر الثورة الرقمية والإلكترونية، وأداة هذا العصر هي وسائل الإتصال الإلكترونية، حيث دخلت هذه الوسائل جميع مجالات الحياة الإنسانية وبشكل قوي وأصبحت أداة للتغيير تستخدمها كافة شعوب العالم في شتى المجالات.

وبإرتباط أجهزة الحاسب بشبكة الإنترنت وإعتماد الناس عليها في أعمالهم المختلفة، وبإحتواء هذه الأجهزة من معلومات مهمة، بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها وتخزنها وتنقلها، فتم التفكير في حماية هذه الأخيرة وحماية المعلومات الموجودة بها من تعرضها لخطر الإختراق والإستيلاء فنشأ مجال الأمن السيبراني وبات من أهم المجالات في عصر التكنولوجيا للحفاظ على هذه الثروة المعلوماتية المهمة.

أصبح الأمن السيبراني يشكل جزءا أساسيا من أي سياسة أمنية وطنية، حيث بات معلوما أن صناع القرار في الدول الكبرى يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية تداركا للمخاطر التي يمكن أن تتعرض لها المعلومات والبيانات في البيئة الرقمية وكذا مختلف الهجمات السيبرانية التي تستهدف المؤسسات الوطنية القائمة على معالجة المعطيات والبيانات المتعلقة بالأفراد. ما استدعى ضرورة وجود ضمانات أمنية ضمن البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني.

سوف نحاول من خلال هذا الفصل تحديد ماهية الأمن السيبراني و كذا الجريمة السيبرانية وذلك بإلقاء الضوء على مفهوم الأمن السيبراني و أهدافه و أبعاده، ثم نعرج إلى الفضاء السيبراني من خلال تبيان الإطار المفاهيمي و فواعله بالإضافة إلى سياسة الفضاء السيبراني في المبحث الأول.

لنتطرق فيما بعد في المبحث الثاني إلى مفهوم الجريمة السيبرانية و صورها و أركانها، و تبيان خصائص المجرم السيبراني و تحديد دوافع ارتكابه لهذا النوع من الجرائم.

المبحث الأول:

مجال و نطاق الأمن السيبرانـــي

يثير موضوع الأمن السيبراني العديد من القضايا القانونية الهامة والتي تؤثر على الحياة العامة والخاصة، فأمن المعلومات يؤثر على حقوق الملكية الفكرية والسرية والخصوصية، وحماية البيانات والحق في حرمة الحياة وعلى هذا النحو، ينقسم هذا المبحث إلى مطلبين؛ حيث يتناول المطلب الأول مفهوم الأمن السيبراني، وأبعاده، ثم يستعرض المطلب الثاني الفضاء السيبراني.

المطلب الأول:

ماهية الأمن السيبرانـــي

أدى التطور التكنولوجي و ما رفقه من ثورة في الإعلام و المعلومات و الإتصالات إلى ظهور مفاهيم حديثة و من أهمها مفهوم الأمن السيبراني، الأمر الذي جعل من موضوعه أهمية كبيرة كونه يعد سلاح إستراتيجيا تسعى خلفه الحكومات والدول لحمايتها من أية إختراق و هذا إستجابة لإدراكهم لحجم التهديدات والتحديات الناتجة عن مخاطر الأمن السيبراني والتي تطال الدولة و مؤسساتها و أفرادها ككل، ولرسم خارطة الطريق نحو تعزيز أمن الفضاء السيبراني بكافة أشكاله.

الفرع الأول/ مفهوم الأمن السيبرانـــي

يعتبر الأمن السيبراني ركيزة أساسية لمجتمع المعلومات، كما يعد دعامة هامة لأنشطة الحكومات والأفراد، و عليه سنتطرق إلى مفهوم الأمن السيبراني فيما يلي:

1- نشأة الأمن السيبرانـــي:

بظهور إستخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينيات من القرن الماضي، ظهرت المعالجة الأولى لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكل هذا الموضوع التساؤل فيما إذا كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة جرمية مستجدة، وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية، فبقيت محصورة في إطار السلوك الأخلاقي دون النطاق القانوني وخلال السبعينيات بدأ الحديث عنها كظاهرة جديدة.[1]

[1] - ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي: دراسة مقارنة، المركز العربي للنشر والتوزيع، القاهرة، الطبعة الأولى، 2017، ص 17.

و قد كانت بداية مفهوم الأمن السيبراني عند تصميم الباحث" روبرت تابان موريس" في سنة 1988 أول برنامج فيروس إلكتروني و التي تعتبر أول دودة حاسوب على الإنترنت حيث تسبب إنتشاره في الأجهزة إلى تعطيل الأنظمة، فحُكِم على موريس بالسجن 03 سنوات و غرامة قدرها 10000 دولار أمريكي، وأصبح أول شخص يدان بموجب قانون الاحتيال وإساءة استخدام الحاسوب، وكان لذلك الحكم دور في تطوير القوانين المتعلقة بالأمن السيبراني.[1]

ليقوم بعدها مخترع البريد الإلكتروني "راي توملينسون" من إختراع برنامج تمكن من خلاله من حذف برنامج الفايروس وصار أول برنامج لمكافحة الفيروسات الإلكترونية، أما في فترة التسعينات وبسبب دخول خدمة الإنترنت الكثير من المجالات و إزدياد عدد المستخدمين للمواقع الإلكترونية، إذ شهدت هذه الفترة تطورا هائلا في مجال الإجرام السيبراني و تغيرا في نطاقها ومفهومها و ظهور أنماط جديدة من الجرائم التي مست العديد من المواقع الإلكترونية أبرزها إختراق موقع البيت الأبيض.[2]

أما في فترة القرن الواحد والعشرين وبسبب إرتفاع عدد مستخدمي الإنترنت ومعدلات الجرائم بالتبعية، وضخامة الخسائر المالية، إنتبهت الكثير من الدول لهذا الخطر الذي يدمر البنى التحتية للمعلومات وتقنية الإتصالات والشبكات، فبدأت الدول تفكر بجدية في إعداد إستراتيجيات للأمن السيبراني لمواجهة الجرائم السيبرانية. [3]

2- تعريف الأمن السيبراني:

أ) السيبرانية إصطلاحا:

جاء مصطلح السيبرانية «Cybernetic» مشتقاً من المصطلح الإغريقي "kyber netes" ويعني الطيار أو قائد الدفة او الحاكم، وتستخدم مجازاً لتعبر عن المتحكم، ويفيد الإشتقاق الحديث بأن كلمة سيبرانية تتضمن آليات تعقيب تتيح وظائف القيادة والتحكم في الأنظمة المغلقة.[4]

والسيبرانية مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي.

وجذور الكلمة الإنكليزية (cyber). متأصل في كثير من الكلمات التي يشيع إستخدامها في مجال تكنولوجيات المعلومات والإتصالات مثل :الفضاء السيبراني "cyber space" والخيال العلمي السيبراني "cyber punk"ويشير قاموس « المورد » إلى السيبرانية بأنها علم الضبط ومصدرها (cybernetics) أي ضبط الأشياء عن بعد والسيطرة عليها .[5]

---

[1] - خالد ظاهر عبد الله جابر السهيل المطري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، المجلد 38، العدد 38، 2022، ص 21.

[2] - فارس محمد العمارات، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، الطبعة الاولى، 2023، ص 33.

[3] - المرجع نفسه، ص 34.

[4] - بيتر بيل سيل، الكون الرقمي: الثورة العالمية في الإتصالات، ترجمة ضياء وراد، هنداوي سي آي سي، 2017، ص 21.

[5] - لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، المجلد 08، العدد 33 -34، 2020، ص 148.

ب) تعريف الأمن السيبراني:

يعرف **الأمن السيبراني** بأنه: مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات الإلكترونية "قراصنة الكومبيوتر" وعواقبها وتنفيذ التدابير المضادة المطلوبة.[1]

كما عرف الأمن السيبراني بأنه" مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية، ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية، وتضم الأهداف العامة للأمن السيبراني ما يلي: التيسر، السلامة التي قد تضمن الإستيقان وعدم الرفض، السرية ".[2]

و قدمت وزارة الدفاع الأمريكية "البنتاغون" أيضاً تعريفا دقيقًا لمصطلح الأمن السيبراني فإعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث "[3]

فالأمن السيبراني مجموعة من الأدوات و السياسات و المفاهيم و الضمانات الأمنية و المبادئ التوجيهية و التقنيات التي يمكن إستخدامها لحماية البيئة الإلكترونية من المخاطر المحدقة بها.

وعليه يمكن تعريف الأمن السيبراني على أنه: مجموعة الوسائل التقنية و التنظيمية و الإدارية التي يتم إستخدامها لمنع الدخول والإستخدام غير المصرح به، و سوء الإستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر وإستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، وإتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.[4]

و عليه فإن الأمن السيبراني هو عبارة عن وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الإتصالات المشفرة.

---

[1] - صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، العدد 62، 2020، ص 277.

[2] - الإتحاد الدولي للإتصالات، شبكات البيانات و الإتصالات بين الأنظمة المفتوحة و مسائل الأمن لمحة عامة عن الأمن السيبراني، التوصية رقم ITU-T X.1205، سنة 2008، ص 2- 3 .

[3] - خالد ظاهر عبد الله جابر السهيل المطري، المرجع السابق، ص 996.

[4] - سمير بارة، الأمن السيبراني (Cyber Security) في الجزائر: السياسات و المؤسسات، المجلة الجزائرية للأمن الإنسانية، جامعة باتنة 1، المجلد02، العدد 02، 2017، ص 258.

3- المفاهيم المرتبطة بالأمن السيبراني:

أ) **الفضاء السيبراني (Cyberspace)** : عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكوّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين، ويُطلق عليه" الذراع الرابعة للجيوش الحديثة."[1]

ب) **الجريمة السيبرانية (Cybercrime)**: هي كل عمل ضار يحدث في الفضاء السيبراني كالإحتيال ونشر محتويات غير قانونية والهجمات التي تستهدف منظومات الإعلام للمؤسسات أو للأفراد بغرض التجسس أو التخريب أو الإبتزاز أو التأثير السلبي على الرأي العام.

ج) **التهديد السيبراني:** هو برنامج ضار آت من الفضاء السيبراني يهدف إلى المساس بأمن الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والشبكات وغيرها من الأشياء المتصلة بالأنترنت. يمكن أن يكون مرتكب التهديد السيبراني شخصا أو دولة أو مجموعة قراصنة أو منظمة ذات أهداف جيوسياسية.[2]

د) **الهجمات السيبرانية (Cyber Attacks)**: أيّ فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أو سياسي، من خلال إستغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام.[3]

هـ) **الردع السيبراني (Cyber Deterrence)**: يعرّف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية.[4]

و) **عمليات الأمن السيبراني:** مجموعة من الإجراءات المرتبطة بإدارة ومراقبة واكتشاف حوادث الأمن السيبراني والتهديدات التي تقع ضمن حيز الفضاء السيبراني ووضع خطط لها وتنفيذها.

ز) **خدمات الأمن السيبراني:** الأنشطة الفنية والإدارية والإستشارية في مجال الأمن السيبراني بما فيها خدمات التقييم الأمني والمراقبة والتدقيق والخدمات الاستشارية.[5]

ي) **الإرهاب السيبراني:** ظهر مصطلح (الإرهاب السيبراني) في الآونة الأخيرة، و عرف بأنه: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، و أن الهجمة يجب أن تكون ذات أثر مدمر و تخريبي مكافئ للأفعال المادية للإرهاب.[6]

---

[1] - إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) مجلة علمية محكمة، جامعة القاهرة، المجلد 12، العدد 3، 2022، ص 724

[2] - ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، الجزائر، المجلد 03، العدد 1، 2022، ص 65.

[3] - نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8، العدد 2، 2018، ص 191.

[4] - إسلام مصطفى جمعة مصطفى، المرجع السابق، ص 725.

[5] - منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، مصر، العدد 111، سنة 2020، ص 11.

[6] - محمد كمال، الإرهاب السيبراني، دار كليم للطباعة و النشر و التوزيع، القاهرة، مصر، الطبعة الأولى، 2022، ص 12.

ل) الحرب السيبرانية: هجوم متعمد بغرض تعطيل عمل أو خداع أو إضعاف أو تدمير أنظمة الكمبيوتر وشبكات الإتصال والمعلومات و البرامج الموجودة في تلك الأنظمة أو الشبكات التي تمر من خلالها.[1]

كما عرفة بأنها إستخدام كل الوسائل السيبرانية من الإختراق والتجسس وتسريب معلومات حساسة بالأمن القومي.[2]

4- أنواع الأمن السيبراني:

وفيما يأتي أبرز أنواع الأمن السيبراني:

أ) أمن الشبكات(Network Security) :

يوفر هذا النوع الحماية لأي من شبكات الحاسوب بأنواعها من أي هجمات، سواء أكانت داخلية أو خارجية بالنسبة للشبكة، وذلك من خلال إستخدام أحدث التقنيات المختلفة لمنع البرامج الخطرة أو سرقة أي من البيانات الأخرى. ويجدر بالذكر أن نوع أمن الشبكات يُستخدم في عدة بروتوكولات مختلفة؛ وذلك لمنع أي من الهجمات الإلكترونية، حيث يسمح فقط للمستخدم المصرح له بالوصول إلى الشبكة الآمنة.[3]

ب) أمن التطبيقات (Application Security):

وهي وضع تدابري لحماية البرامج من الفيروسات الضارة وعدم سرقة المعلومات السرية، وذلك بالسعي إلى إفشال أي نوع من الهجمات على الأمن السيبراني بواسطة إستخدام العديد من الأجهزة والبرامج خلال مرحلة تطوير المشروع الإلكتروني، ومن خلال هذا النوع تستطيع الشركات أو المؤسسات اكتشاف مجموعة البيانات الحساسة، والتي يجب حمايتها بشكلٍ كبير.[4]

ج) الأمن السحابي (Cloud Security):

يعد الأمن السحابي تقنية سيبرانية تعتمد على ضغط المعلومات وهو جزء لا يتجزأ من الأمن السيبراني و يعرف الأمن السحابي بأنه سياسات وتقنيات وضوابط تعمل جميعها لحماية البيانات المنتشرة والتطبيقات المرتبطة بها والمكونة للحوسبة السحابية، واجبها حماية البيانات والفصل بين الواجبات وأمن التطبيقات والأنظمة السرية وغيرها من الواجبات، حيث تُمَكن المستخدمين من تخزين البيانات ومراقبتها وذلك بإستخدام تطبيق الأمن السحابي.[5]

---

[1] - شادي عبد الوهاب منصور، حروب الجيل الخامس، العربي للنشر و التوزيع، الطبعة الأولى، 2019، ص 99.

[2] - علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، الطبعة الأولى، 2022، ص 103.

[3] - منى عبد الله السمحان، المرجع السابق، ص 14.

[4] - مسيكة محمد، الفضاء السيبراني وتحديات الأمن القومي للدول، جملة العلوم القانونية والإجتماعية، المجلد 07، العدد 04، 2022، ص 458.

[5]- إسراء شريف جيجان، الأمن السيبراني الصيني: دراسة في الدوافع والتحديات، مجلة قضايا سياسية، جامعة النهرين، العدد 65، 2022، ص 38.

الفرع الثاني/ أهداف و عناصر الأمن السيبراني:

يسعى الأمن السيبراني جاهدا لضمان تحقيق سلامة المؤسسات و الأفراد في مواجهة الأخطار السيبرانية المحدقة بهم في الفضاء السيبراني و تتمثل أهداف و عناصر الأمن السيبراني فيما يلي:

1- أهداف الأمن السيبراني:

من أهم أهداف الأمن السيبراني ما يلي:

1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
2- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
3- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
4- صمود البني التحتية الحساسة للهجمات الإلكترونية.
5- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين
6- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة بإختلاف أنواعها.
7- سد الثغرات في أنظمة امن المعلومات.
8- مقاومة البرمجيات الخبيثة، وما تستهدفه من أحداث أضرار بالغة للمستخدمين.
9- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
10- إتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات إستخدام الإنترنت المختلفة.
11- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة بإختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.[1]

2- عناصر الأمن السيبراني:

حتى يتحقق الهدف من الأمن السيبراني، لابد من توافر مجموعة من العناصر تعمل مع بعضها البعض لتكمل الدور في ذلك، و من أهم عناصر الأمن السيبراني:

[1] - منى عبد الله السمحان، المرجع سابق، ص 12.

أ) التقنية:

تشكل التكنولوجيا و التقنية دورا في غاية الأهمية في حياة الأفراد و المنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، و تشمل حماية الأجهزة بمختلف أشكالها الذكية و الحاسوبية و الشبكات بالإعتماد على جدران الحماية و إستخدام برامج مكافحة الفيروسات و غيرها.[1]

ب) الأشخاص:

يستوجب على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما إستخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، بالإضافة إلى تفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ إحتياطية للبيانات. [2]

ج) الأنشطة والعمليات (Process):

يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.[3]

الفرع الثالث / أبعاد الأمن السيبراني:

يرتبط الأمن السيبراني بمجالات عديدة و مختلفة منها:

أ) الأبعاد العسكرية:

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف ال قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي إختراق خارجي قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تجسس على أمن العسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الإتصال في ما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية فقدان السيطرة على وحدات القيادة.[4]

---

[1] - فارس محمد العمارات، إبراهيم الحمامصة، المرجع السابق، ص 36.
[2] - المرجع نفسه، ص 36.
[3] - نفس المرجع، ص 37.
[4] - منى عبد الله السمحان، المرجع السابق، ص 15

ب) الأبعاد الاقتصادية:

يرتبط الأمن السيبراني إرتباطاً وثيقاً بالإقتصاد، فالتلازم واضح بين إقتصاد المعرفة وتوسع إستخدام تقنيات المعلومات والإتصالات والتي تتيح تعزيز التنمية الإقتصادية لبلدان كثيرة عبر إفادتها من فرص الإستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط، إلا أن هذا الواقع يطرح مسائل مختلفة سواء ما تعلق بحماية مقدم الخدمة والعمل أو بحماية المستهلك عبر الإنترنت.

ضف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد إستثمارات المصارف والمؤسسات المالية في مجال المال الرقمي.

حيث أن حجم التجارة الإلكترونية بلغ تريليونات دولار الذي تعد مبالغ كبيرة للتداول في ظل إنتشار و إرتفاع معدل الجرائم السيبرانية المنظمة والخطيرة، فإن ذلك يمثل تهديداً صريحاً لنمو الإقتصاد الرقمي ما لم تقم الدول بتعظيم معايير الأمن السيبراني بما يضمن الحد من هذه الجرائم.[1]

ج) الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لإستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جداً على المستوى الخارجي والدولي، كما أنه لا أحد يُنكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي مثل: حملات إنتخابية، تظاهرات افتراضية، حركات إحتجاجية إلكترونية، كما يتم إستغلال هذه المواقع من طرف العديد من الحكومات لتمريرها.[2]

د) الأبعاد القانونية:

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومع ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

---

[1] - فارس قوة، الأمن السيبراني - Cyber Security، الموسوعة السياسية، رابط الموقع:
https://political-encyclopedia.org/dictionary/الأمن%20السيبراني

[2] - منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، جامعة الدول العربية، القاهرة ،2016، ص 29.

إن سن التشريعات الملائمة يشجع المستثمرين و الشركاء الإقتصاديين على الإستثمار كونه يعزز الثقة لديهم بإنشاء بنية تحتية سليمة وموثوقة خالية من الإختراقات، لأن الأمن المعلوماتي القائم على أساس الثقة والجودة يضع الأسس الصحيحة والسليمة لإقتصاد خدمات سليم.[1]

هـ) الأبعاد الاجتماعية:

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على إستقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن إنفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل.[2]

وفي الأخير يمكن القول إن الأمن السيبراني هو بُعد جديد ضمن أبعاد الأمن القومي، أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية كالصراع والقوة والتهديد، حيث حتّم على فواعل المجتمع الدولي الإنتقال من عالم مادي إلى عالم إفتراضي في غاية التعقيد والتشابك .وبالتالي أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل إرتباط كافة التفاعلات الدولية بالجانب الرقمي والتكنولوجي، الأمر الذي يستدعي على الدول ضرورة إيجاد ميكانيزمات ووسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثمة تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي.

المطلب الثاني:

مفهوم الفضاء السيبراني

بفضل ثورة المعلومات، ومع ظهور الأنترنت ومواقع الويب ظهرت بيئة جديدة أخرى وهي الفضاء الإلكتروني، إذ تختلف عن البيئات الأربعة الطبيعية " البر، البحر، الجو و الفضاء الخارجي " في كونها بيئة من صنع الإنسان، كما أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بضفة عامة و الحياة البشرية بصفة خاصة.

الفرع الأول / الإطار المفاهيمي للفضاء السيبراني

يعد الفضاء السيبراني المجال الحيوي الجديد الناتج من التطورات التقنية والتكنولوجية الحديثة، و بالتالي يمكن تحديد الإطار المفاهيمي للفضاء السيبراني فيما يلي:

[1] - أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات و التخطيط، 2016، ص 9.
[2] - محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر و التوزيع، 2020، ص 36-38

1- مفهوم الفضاء السيبراني:

يخلط البعض بين الفضاء السيبراني أو ما يعرف بالفضاء الإلكتروني والأنترنت، في حين أن الأنترنت هو الوسيط الذي تقوم من خلاله بتلبية جميع الأغراض المتعددة والعديد من الخدمات المتاحة على الأنترنت؛ ولكن الفضاء الإلكتروني أبعد من ذلك على الرغم أن بنيته أساسها الإنترنت، ولكنه أكثر ثراء؛ وأصبح الفضاء الإلكتروني والإنترنت مجتمعا يتفاعل فيه المواطنين عن طريق الشبكات، ولا يوجد خط فاصل بين الفضاء الإلكتروني و الإنترنت، ولكن معيار التفرقة، يكون بحكم الخبرة والتعاملات والفئة العمرية.[1]

أ- تعريف الفضاء السيبراني:

الفضاء السيبراني (cyberspace) مصطلح حديث ظهر نتيجة لثورة تكنولوجيا المعلومات و يشمل جميع الحواسيب و المعلومات التي بداخلها و الأنظمة و البرامج و الشبكات المفتوحة للإستعمال الجمهور العام أو تلك الشبكات التي صممت لإستعمال فئة محددة من المستعملين، حيث عرفت الوكالة الفرنسية لأمن أنظمة الإعلام و المكلفة بالأمن السيبراني الفرنسي الفضاء السيبراني بأنه: "فضاء التواصل المشكل من خلال الربط البيني لمعدات المعالجة الآلية للمعطيات الرقمية "[2].

و إستخدمت كلمة "cyberspace" للتعبير عن الإنترنت في عام 1991، غير أنه أصبح هذا المفهوم أشمل و أوسع من الإنترنت ليضم كل الإتصالات و الشبكات و قواعد البيانات و مصادر المعلومات، و أصبحت بنية النظام الإلكتروني تعني المكان الذي لا يعد جزءا من العالم المادي أو الطبيعي حيث أنها ذو طبيعة إفتراضية رقمية إلكترونية تتحرك في بيئة إلكترونية حيوية و تعمل من خلال خطوط الهاتف و كابلات الإتصال و الألياف البصرية و الموجات الكهرومغناطيسية.[3]

الفضاء السيبرانيّ هو تلك البيئة الافتراضيّة التي تعمل فيها المعلومات الإلكترونيّة والتي تتّصل عن طريق شبكات الكمبيوتر الفضاء السيبرانيّ، مثل الفضاء التقليديّ، يتألّف من أربعة مكوّنات رئيسيّة؛ هي المكان، والمسافة، والحجم، والمسار.[4]

كما عرف "جوزيف ناي" الفضاء الإليكتروني بأنه نطاق تشغيلي مُحكم بإستخدام الإليكترونيات لإستكشاف المعلومات عبر أنظمة مترابطة ببعضها البعض وببنيتها التحتية.[5]

---

[1] - لورنس لسيج، الكود المنظّم للفضاء الإلكترونية، ترجمة :محمد سعد طنطاوي، مؤسسة هنداوي للتعليم والثقافة، القاهرة، طبعة 02، 2006، ص 31.

[2] - علاء الدين فرحات، الفضاء السيبراني : تشكيل ساحة المعركة في القرن الحادي و العشرين، مجلة العلوم القانونية و السياسية، جامعة الشهيد حمه لخضر الوادي، المجلد 10، العدد 03، 2019، ص 90.

[3] - عادل عبد الصادق، الفضاء الالكتروني والرأي العام. تغير المجتمع والادوات والتأثير، قضايا استراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة، 2009، ص 8.

[4] - محمود بري، السيبرنيطيقا (السيبرانية)علمُ القُدرة على التوَاصُل والتَّحكُّم والسَّيطرة، المركز الإسلامي للدراسة الإستراتيجية، بيروت، لبنان، الطبعة الأولى، سنة 2019، ص 16.

[5] - إيهاب عبد الحميد خليفة، الفضاء الإلكتروني وتهديدات الأمن القومي المصري، المركز العربي لأبحاث الفضاء الإلكتروني،2013، تم تصفح الموقع بتاريخ: 2023/02/06، على الرابط: http://www.accronline.com/print_article.aspx?id=15383

كما جاء تعريف الإتحاد الدولي للإتصالات للفضاء الإلكتروني بأنه: " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمي كل هذه العناصر".[1]

يمكننا القول إن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، ومكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين، سواء كانوا مشغلين أو مستعملين". وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء السيبراني" هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات، كل بحسب رؤيته وإستراتيجيته وقدرته على إستغلال المزايا المتاحة، ومواجهة المخاطر الكاملة في هذا الفضاء.[2]

ب- مكونات الفضاء السيبراني:

-**الأجهزة (Hard Ware)** : وتعرف على إنها الجزء المادي لتكنولوجيا المعلومة المتمثل بالحواسيب والأجهزة الملحقة بها لتنفيذ المهام المطلوبة .

-**الإنترنت (Internet)** : ويعرف على إنه الترابط الهائل لشبكات الحاسوب ذات النطاق العالمي التي تمكن الاتصال بين البرامج التكنولوجية المتباينة، أو إنه نظام الحواسيب الذي يربط معاً (تشابك) في النظام ليسمح بتبادل المعلومات والمصادر، وإن استخدام الحواسيب المرتبطة بواسطة وسائل الاتصالات (مثل الهواتف) يجعل سهولة تواصل كل الأفراد عبر العالم . [3]

-**البرمجيات (Software)**: وتتألف برمجيات الحاسوب من تعليمات مبرمجة ومفصلة بهدف السيطرة والتنسيق على مكونات الأجهزة المادية في نظام المعلومات والبرمجيات هي برامج الحاسوب التي تحكم عمل المكونات المادية وتتولى مهام تطبيقات مختلفة.[4]

-**الشبكات (networks)** : وهي عبارة عن مجموعة من الحواسيب تنظم معاً وترتبط بخطوط إتصال بحيث يمكن لمستخدمها المشاركة في الموارد المتاحة ونقل تبادل المعلومات فيما بينها، وتستخدم هذه الشبكات لتحقيق مجموعة من الأغراض مثل: توفير الاتصال بين الأشخاص والوصول للمعلومات عن بعد والتجارة الإلكترونية وتخفيض المصروفات، وهناك عدة أنواع من الشبكات منه: الشبكات المحلية (LAN) ، شبكة المنطقة (MAN)، الشبكات الواسعة.[5]

- **المعلومات و البيانات:** يتكوّن الفضاء السيبراني كذلك من المعلومات و البيانات المخزونة فيه و التي تنتقل من خلال شبكات الإتصال. [6]

---

[1] - محمود علي عبد الرحمان، أسامة فاروق مخيمر، الفضاء الالكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، جامعة بني سويف، مصر، المجلد 16، العدد 15، 2022، ص 428.

[2] - حازم محمد خليل، إستغلال الفضاء السيبراني في الحروب غسر التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية بجامعة الإسكندرية، المجلد 08، العدد 25، 2023، ص 269.

[3]- خلود عاصم ومحمد ابراهيم، دور تكنولوجيا المعلومات والاتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية الجامعة، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص 233

[4] - غسان قاسم داود، تحليل مكونات البنية التحتية لتكنولوجيا المعلومة دراسة استطلاعية في بيئة عمل عراقية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص 11.

[5] - تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، العدد 33 – 34، السنة الثامنة، 2020، ص 151.

[6] - محمود بري، المرجع السابق، ص 50.

2- طبقات الفضاء السيبراني: يتكون هذا الفضاء الرقمي من ثلاثة طبقات:

أ) الطبقة المادية: وهي تمثل كل ما هو مادي كالمنشآت والشبكات والميكروكمبيوتورات والخوادم والأشياء المتصِلة بالإنترنيت...الخ. تكوّن هذه الطبقة مجالا للحروب الإلكترونية.

ب) الطبقة المنطقية وهي تشمل أنظمة الإستغلال والتطبيقات والبروتوكولات...الخ. تمثل هذه الطبقة مجالا للحروب السيبرانية.[1]

ج) الطبقة السيميولوجية: وهي تتكون من كل المحتويات بيانات ومعلومات ورسائل...الخ التي يطلع عليها مستعملي الفضاء السيبراني أو يتبادلونها. تعتبر هذه الطبقة مجالا للحروب النفسية أو المعلوماتية.[2]

الفرع الثاني/ فواعل الفضاء السيبراني:

تتكون تركيبة الفواعل في الفضاء السيبراني من مستويين، الأول على المستوى الدولاتي، أما الثاني فهو على المستوى اللادولاتي.

1- **الفواعل الدولاتية:** وهنا نشير أساسا إلى الإحتكار القانوني والمُنظم للدولة للفضاء الافتراضي من خلال مختلف أجهزتها (وزارات، وحدات الأمن...الخ)، حيث تعد الدولة فاعل محوري في تسيير الفضاء الإفتراضي إنطلاقا من إمكاناتها المادية والبنيوية و البشريةٌ والقانونية ولذلك لابد للدولة من التحكم في مجال الفضاء السيبٌراني، وهو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى، التي قد تصل حد تهديد مصالح الدولة نفسها، بل وممارسة كل أنواع الحروب النفسية الإفتراضية على مواطنيها.[3]

2- **الفواعل اللادوالاتية:** هنا يأتي دور الأفراد والجماعات والمنظمات غير الحكومية والشركات اللذين أصبحوا بإمكانهم التحكم في توجهات الدول وإدارتها وفق سياسات معينة من خلال الفضاء السيبراني، ومن أهم هذه الفواعل ما يلي:

أ) **الفرد:** أصبح الفرد فاعلا مهما في الفضاء السيبراني حتى أن له القدرة على إحداث الثورة الرقمية، وتصبح تلك الثورة مجال إستخدام للدولة نفسها، ومثال ذلك مواقع التواصل الإجتماعي وعلى رأسها موقع" الفيسبوك" الذي يستقطب أكثر من مليار مستخدم عبر العالم.

ب) **المنظمات غير الحكومية:** تعتمد هذه المنظمات بشكل كبير على شبكة الانترنت ووسائل التكنولوجيا الحديثة في تعبئة الرأي العام، والضغط على الحكومات من خلال ترتيب الحملات الإجتماعية وتعبئة المجتمع المدني من أجل الضغط على الحكومات للتغيير في سياسات معينة، مثل ما تقوم به اليوم معظم منظمات البيئة العالمية فيما يخص إتفاقيات التغير المناخي.[4]

---

[1] - ساعد بوقرص، المرجع السابق، ص 63.

[2] - المرجع نفسه، ص 64.

[3] - سهام حسن علي الشمري، تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية، جامعة بغداد، العدد 83، 2020، ص 146.

[4] - محمد محمود العمري، المرجع السابق، ص 33.

ج) **الشركات متعددة الجنسيات:** تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكرا على الدول، فخوادم شركات مثل: جوجل (Google)، و فيسبوك(Facebook)، و مايكروسوفت(Microsoft)، تحتوي على كم هائل من البيانات و المعلومات والتي تسمح لها بالتأثير على الأسواق و إقتصاد الدول و ثقافة المجتمعات و توجهاتها. [1]

حيث تسعى الشركات الكُبرى نحو الإستثمار في البيانات الشخصية، فهي ثروة تعيش عليها الشركات، التقنية منها، والتقليدية، نتيجة إستخدامها في مجال تطوير المنتجات، والإعلانات، عبر تحليلها، وتحليل ميول الأشخاص الطبيعيين، وتحديد حاجاتهم، وعاداتهم الإستهلاكية، وإهتماماتهم.[2]

د) **المجموعات الافتراضية:** هنا يأتي دور القراصنة (HACKERS) وغالبا ما يسعون لتحقيق أهداف مختلفة مالية، مادية، سياسية، إيديولوجية ...إلخ، ومثال ذلك نجد المجموعة الافتراضية المشهورة (Anonymous)، والتي تسعى لتسويق خطابات ومطالب سياسية في العالم، و كذا القيام بعمليات القرصنة السيبرانية و سرقة المعلومات و إختراق الحسابات البنكية و تحويل الأموال، كما توجد سوق سوداء لكل ما هو غير مشروع عبر الإنترنيت المظلم (Dark internet).[3]

هـ) **الجماعات الإرهابية:** حيث أصبحت هذه الفئة تعتبر من أبرز الفواعل التي تلجأ إلى الفضاء السيبراني للقيام بعمليات التجنيد و التعبئة و الدعاية و جمع الأموال و التواصل مع عناصرها في أماكن و دول مختلفة، بالرغم من أنها لم تصل بعد إلى مرحلة القيام بهجمات سيبرانية حقيقية على المنشآت و البنى التحتية للدول.[4]

الفرع الثالث/ سياسة الفضاء السيبراني

للفضاء السيبراني سياسات مختلفة طبقا للإستراتيجيات التي تعتمد عليها الفواعل الدولاتية فيه و تتمثل سياسة الفضاء السيبراني في:

1- الفضاء السيبراني المفتوح:

ويمثله كلا من الإتحاد الأوروبي و الولايات المتحدة الأمريكية، إذ نشأت في الأصل في الولايات المتحدة مع نشوء الانترنت وتقوم على الحرية وعدم اخضاع الانترنيت لأي سلطة، بل أن نشوء الفضاء كان للهروب من رقابة الدولة، إذ سمي بأنه الفضاء الرابع والفكرة الأساسية هو فضاء بلا حدود يضمن التدفق الحر للمعلومات. وظهر إعلان حرية الإنترنت عام 1998.

---

[1]- علي محمد منيف الرفيعي، تحديات الأمن في الفضاء السيبراني الأمريكي، مجلة دراسات دولية، جامعة بغداد، المجلد 20، العدد 85، 2021، ص 295.

[2] - منى الأشقر جبور، البيانات الشخصية والقوانين العربية الهمّ الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت، لبنان، 2018، ص 12.

[3] - سهام حسن علي الشمري، المرجع السابق، ص 147.

[4] - محمد محمود العمري، المرجع السابق، ص 34.

وهذه السياسة تقوم على حيادية الفضاء الرقمي وهي تضع حقوق الإنسان وحرياته ضمن أولويات الدولة، والاستثناء هو تقييدها لمقتضيات الأمن العامة، وهي وإن كانت تعطي الأولوية للأمن إلا أنها تعطي منزلة مساوية له هي إحترام حرية التعبير والخصوصية، فالأمن لا يمكن أن يكون مبررا لتقييد الحرية إلا في حالات خاصة.[1]

وتقوم هذه السياسة على ثلاثة (3) مبادئ:

أ) مبدأ الضرورة (Necessity): أي أن الأصل هو إحترام الخصوصية، وحماية الأمن الوطني هي الضرورة التي تبيح تدخل الدولة في رقابة نشاطات؛ لذلك تم إبطال عدد من قوانين الإتحاد الأوروبي؛ لأنها جاءت خالية من الضرورة.

فعلى سبيل المثال ألغت المحكمة الأوروبية لحقوق الإنسان الأمر التشريعي الصادر عن الإتحاد الأوروبي رقم (24) لسنة 2006 والذي ألزم الشركات بضرورة الإحتفاظ بالمراسلات الإلكترونية للأفراد لمدة ستة (06) أشهر والسماح للجهات الأمنية بالإطلاع عليها، وقد جاء في قرار المحكمة أن الأمر التشريعي يتضمن إمكانية الوصول لأسماء وعناوين ومراسلات وتنقلات المستخدمين الإلكترونية، وهذه البيانات جزء من الخصوصية التي يجب ضمانها، لذلك فإن الأمر التشريعي يمثل تجاوزا كبيرا على حقوق الانسان الأساسية المتمثلة بالحق في الخصوصية والحق في حماية البيانات الشخصية .[2]

ب) مبدأ تحديد المدة (temporary measures): أي أن تنفيذ إجراءات رقابة حسابات الأفراد تسري لمدد معينة وتكون بحاجة للتجديد السنوي مع ضرورة موافقة السلطة التشريعية عند التجديد، وهي حالات الطوارئ التي تنظمها الدساتير الوطنية، وهذا الشرط ينطبق على جميع حالات الدخول غير المصرح به من قبل أجهزة الدولة الأمنية لحسابات الأفراد من قبل الجهات الأمنية لمنع الجرائم التي تمس أمن الدولة.

ولعل أكبر مثال على ذلك هو قانون مكافحة الإرهاب الأمريكي المعروف بإسم (Act patriot) بعد تفجيرات برجي التجارة العالمي في 11 سبتمبر 2001، إذ أن أغلب نصوصه إنتهت عام 2004، لكن تم تجديد البعض منها لسنة أو سنتين، وهو حاليا قد أوقف تنفيذه.[3]

ج) مبدأ الرقابة القضائية (judicial review): ويعني أن جميع أعمال الحكومة تخضع لرقابة القضاء، وتدخّل القضاء يكون بشكلين، سابق ولاحق، السابق يقتضي الحصول على أمر قضائي للحصول على المعلومات الشخصية، واللاحق يعني إمكانية الطعن بإجراءات الأجهزة الأمنية أمام المحكمة المختصة، وهذه

[1] - سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني دراسة في ضوء احكام القانون الدولي العام، مجلة لارك للفلسفة و اللسانيات و العلوم الاجتماعية، العدد 46، مجلد 3، سنة 2022، ص 527

[2] - المرجع نفسه، ص 528.

[3] - نفس المرجع، نفس الصفحة.

تعد ضمانات تصعب على الأجهزة الأمنية أن تسيئ إستغلال سلطتها بالمساس بحق الخصوصية و سرية المعلومات الشخصية.[1]

2-الفضاء السيبراني المتحكم فيه:

و يمثله كلا من الصين و روسيا الإتحادية، وتقوم هذه السياسة على إخضاع الفضاء السيبراني لسيادة الدولة، اذ هو في نظرهم إمتداد للتلفاز والبث الراديوي، لذلك تحاول تلك الدول إبراز فكرة سيادة الدولة على الفضاء السيبراني وترى أن لكل دولة الحق في تنظيم فضائها الإلكتروني .

ويسود في هذا الإتجاه تعظيم المخاطر الأمنية وإعطاء التهديدات الأمنية إهتمام أكبر بكثير من حماية الحريات الفردية، إذ تبنت دول الاتحاد ما يسمى بمبدأ (أمن المعلومات) الذي صاغته روسيا الإتحادية مع بداية عام 2000، ويعني أن حماية الأمن الوطني هو الأولوية القصوى عند تنظيم الفضاء السيبراني.[2]

و يعرف هذا النظام الروسي المسمى بـ (SORM ||) وهو نظام مراقبة النشاطات الذي تم المصادقة عليه في روسيا الإتحادية وأصبح نافذا اعتبارا من عام 2000 ،ويرتكز على إلزام جميع مزودي الإنترنيت بتثبيته في برامجهم، وهو يقوم بتسجيل كافة النشاطات على الإنترنت مع عناوين المستخدمين ووقت النشاط.

وهذا الإتجاه يخول الجهات الأمنية سلطات شبه مطلقة في التعامل مع البيانات الخاصة للأفراد من غير حاجة لإستحصال أمر قضائي، كما لا توجد جهة رقابية أعلى من تلك الجهات الأمنية من الممكن أن تراقب عملها وتمنع إستغلالها للسلطات الواسعة الممنوحة لها.[3]

ويقوم هذا الإتجاه على ثلاثة(03) مبادئ:

أ) **مبدأ التوطين (localisation data):** وهذا المبدأ يتعلق بعدم السماح بمعالجة البيانات التي تخص الدولة ورعاياها في مزود خدمة يقع خارج حدود الدولة، وهي تفرض على شركات مزودي خدمة الإنترنت وكذلك شركات التواصل الإجتماعي مثل الفيسبوك و الواتس اب وشركة غوغل أن يتم تخزين جميع تلك المعلومات في ذاكرة سحابية ضمن إقليم الدولة ذاتها.

ب) مبدأ الرقابة (surveillance): ويعني أن الأجهزة الأمنية في الدولة تستطيع في أي وقت الدخول للبيانات الشخصية لمستخدمي الإنترنت، كما أن شركات خدمة الإنترنت ملزمة بالاحتفاظ بمراسلات مستخدمي الإنترنت لمدة لا تقل عن 06 أشهر وتمكين الأجهزة الأمنية من الإطلاع عليها في أي وقت.

[1] - سامر محي عبد الحمزة المرجع السابق، ص 529
[2] - المرجع نفسه، نفس الصفحة.
[3] - نفس المرجع، ص530.

وتتمتع أجهزة الأمن الروسية والصينية بصلاحية الدخول على البيانات الشخصية للأفراد من غير حاجة إلى إستصدار أمر قضائي ومن غير أن تخضع لرقابة أي سلطة أعلى منها في هذا الشأن، إذ أن الخصوصية ليست محل إعتبار أمام حماية الأمن العام.[1]

ج) مبدأ الفلترة (Censorship): وهو حجب المواقع الإلكترونية والبرامج جزئيا أو كليا إذا رأت ذلك ضرورة لحماية الأمن الوطني، وقد يصل الأمر إلى عزل الدولة بالكامل عن الشبكة العالمية، وهو المشروع الذي تعمل عليه روسيا الإتحادية حاليا.

والفلترة تتم أيضا من غير إشتراط موافقة جهة معينة، بل هي سلطة تقديرية لثلاثة (03) جهات وهي: الجهات الأمنية، والمدعي العام، والهيئة الفدرالية المشرفة على الإتصالات وتكنولوجيا المعلومات ووسائل الإعلام العامة.

وتطبيق هذا النظام يتناقض مع العديد من الحقوق والحريات المقررة بالمواثيق الدولية مثل الحق في التعبير عن الرأي والحق في الخصوصية، و كذا تقييد حرية التعبير ومنع إنتقاد الدولة و أدائها.[2]

المبحث الثاني:

ماهية الجرائم السيبرانية و دوافع إرتكابها

يشهد المجتمع اليوم تطوراً متسارعاً لتكنولوجيا المعلومات والاتصالات، كما يشهد تزايداً وتنوعاً في التطبيقات والخدمات الإلكترونية التي تعتمد أساساً على الفضاء السيبراني، إلا أن الإنفتاح الذي يميز الإنترنت و الفضاء السيبراني عموما جعله عرضت للتعديات و الإنتهاكات و الأنشطة الإجرامية و التعدي على حقوق الناس، وجعل من مستخدمي الفضاء السيبراني عرضة للإنتهاكات من قبل المجرمين و مخترقي الشبكات، مما يؤثر سلبا على جميع المستخدمين من أفراد و شركات مؤسسات حكومية و منظمات.

المطلب الأول:

الإطار المفاهيمي للجرائم السيبرانية

يعتبر مصطلح "الجريمة السيبرانية" من المصطلحات غير القابلة لمدلول أحادي، و هذا ناتج عن التطورات الحديثة و المستمرة في مجال الحاسب الآلي و الأنترنت و التي من بينها: جرائم الحاسوب و الإنترنت، جرائم التقنية العالية، الجريم الإلكترونية، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وصولا إلى الجرائم السيبرانية. [3]

---

[1] - سامر محي عبد الحمزة، المرجع السابق، ص 530.

[2] - المرجع نفسه، ص 531.

[3] - حسنين شفيق، الاعلام الجديد و الجرائم الإلكترونية، التسريبات، التجسس، الإرهاب الإلكتروني، دار فكر و فن للطباعة و النشر و التوزيع، 2014، ص 17.

الفرع الأول/ مفهوم الجريمة السيبرانية:

تعد الجرائم السيبرانية من الجرائم المستحدثة و التي تتطور بشكل مستمر بتطور تكنولوجيا الإعلام و الإتصال و عليه سنعالج مفهوم الجريمة السيبرانية فيما يلي:

أولا/ تعريف الجريمة السيبرانية:

تعددت التعاريف للجريمة السيبرانية و جاءت حسب إتجاهات و وجهات نظر مختلفة و ذلك راجع لحداثة المفهوم عالميا، فمن التعريفات ما يركز على إستخدام الحاسب كوسيلة و أداة للجريمة ومنها ما يركز على موضوع الجريمة أي أنها تقع على مكونات الحاسب كالبيانات و البرامج، و منها ما يشترط أن يكون للمجرم معرفة فنية تمكنه من فعل الجريمة، ومنها ما جمع في التعريف بين الوسيلة و الموضوع. [1]

حيث عرفها الفقيه الألماني "تاديمان: " هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب بإستخدام الحاسب الآلي ".

كما يعرفها الخبير القانوني "جون فورستر" بأنها: "كل فعل إجرامي يستخدم الكمبيوتر في إرتكابه كأداة رئيسية ". [2]

كما تعرف بأنها:" مجموعة من الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية".[3]

إذ إستخدم مصطلح "cyber crime" مثل ما جاءت به إتفاقية المجلس الأوروبي "إتفاقية بودابست" تحت عنوان " convention on cyber crime " حيث إعتبر هذا المصطلح شاملا للجرائم المعلوماتية وجرائم الشبكات. [4]

فالجريمة السيبرانية هي: كل ما يقع على الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها (الأجهزة والبرمجيات والخدمات) من إختراق أو تعطيل أو تعديل أو إستخدام أو إستغلال غير مشروع.

ومن جهة أخرى هي: الجريمة التي يكون النظام المعلوماتي فيها وسيلة الإرتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الإنترنت[5].

---

[1] - عادل عبد العزيز صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، دار كنوز إشبيليا للنشر و التوزيع، الرياض، المملكة العربية السعودية، الطبعة الأولى،2017، ص 24.

[2] - محمد محمود العمري، المرجع السابق، ص 42.

[3] - محمود مدين، فن التحقيق والإثبات في الجرائم الالكترونية، المصرية للنشر والتوزيع، الطبعة الأولى، 2020، ص 29.

[4] - أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية و الأجنبية، مكتبة القانون و الإقتصاد، الرياض، الطبعة الأولى، 2014، ص 91.

[5] - جيلالي دلالي، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، 2021، ص 538.

كما عرفها المشرع المغربي في المادة 02 فقر02 من القانون 20-05 المتعلق بالأمن السيبراني بأنها:" مجموعة من الأفعال المخالفة للتشريع الوطني أو الاتفاقيات الدولية التي صادقت عليها المملكة المغربية، التي تستهدف شبكات ونظم المعلومات أو تستعملها كوسيلة لارتكاب جنحة أو جناية."[1]

كما عرف المشرع الأردني الجريمة السيبرانية في المادة 02 من القانون رقم 16 المتعلق بالأمن السيبراني لسنة 2019 بأنها:" الفعل أو الهجوم الذي يشكل خطرا على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها و يتطلب إستجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه".[2]

في حين نص المشرع الجزائري على الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في قانون رقم 09-04 و عرفها في المادة 02 الفقرة أ منه بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية".[3]

وعليه نستنتج أن المشرع الجزائري تبنى معيار النظام المعلوماتي لتحديد معالم الجريمة السيبرانية تاركا المجال واسعا لأية جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.[4]

ومع ذلك فقد تباينت التعاريف المقدمة للجريمة السيبرانية تباين المقاربة المعتمدة في هذا المجال، ما بين:

أ- **مقاربة لغوية:** دلالية تركز على العلاقة بين هذه الجرائم وفضاء المعلوماتية العابر للحدود المتسع لإرتكاب الكثير من الجرائم.

ب- **المقاربة الجنائية:** المهتمة بدراسة الظاهرة الإجرامية، و أساسُها أنَّ تقنيات المعلومات الحديثة تسهل وتوسع نطاق و تزيد من خطورة بعض الجرائم التقليدية السابقة على إكتشاف هذه التقنيات بالإضافة إلى ظهور جرائم جديدة مرتبطة بظهور هذه التقنيات.

ج -**المقاربة القانونية:** و مفادها أن الجرائم المرتكبة بواسطة تقنيات الإعلام و الإتصال تدخل في نطاق الإجرام المعلوماتي، و هي أساسا نوعان؛ جرائم تستهدف الشبكة و جرائم تُرتكب بواسطتها.[5]

---

[1] - قانون رقم 20-05 مؤرخ بتطوان في 4 ذي الحجة 1441 (25 يوليو 2020)، المتعلق بالأمن السيبراني، الجريدة الرسمية للمملكة المغربية، عدد 6904، الصادر في 9 ذي الحجة 1441 (30 يوليو 2020).

[2] - قانون رقم 16 لسنة 2019، الامن السيبراني، الجريدة الرسمية للملكة الاردنية الهاشمية، عدد 5595، الصادرة في 16 سبتمبر 2019.

[3] - قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، جريدة رسمية للجمهورية الجزائرية، عدد 47، الصادرة في 25 شعبان 1430 الموافق لـ 16 غشت 2009.

[4] - ميرفت محمد حبايبة، مكافحة الجرائم الالكترونية - دراسة مقارنة - في التشريع الجزائري والفلسطيني، دار اليازوري العلمية للنشر و التوزيع، الأردن، 2022، ص 39.

[5] - سيدي محمد الأمين الراظي، الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي و الدولي، مجلة القانون و الأعمال الدولية، مقال منشور في 22 يوليو 2019، رابط الموقع: https://www.droitetentreprise.com/الجريمة-السيبرانية-وتكاملية-النص الو

ثانيا/ خصائص الجريمة السيبرانية: تتميز الجريمة السيبرانية بمجموعة من الخصائص و من أبرزها ما يلي:

1- الطابع الدولي لجرائم السيبرانية (عابرة للدول و القارات):

يعد الطابع الدولي للجريمة السيبرانية من أبرز خصائصها و هي بذلك تتحدى النظام القانوني المحلي و الدولي، إذ يطغى في كثير من الأحيان الطابع الدولي على الجريم السيبرانية، فهي جريمة عابرة للحدود، و قد تتضمن أكثر من عنصر أجنبي، فالفعل الجرمي قد يحصل في بلد معين، وتتحقق النتيجة الجرمية في بلد آخر أو في مجموعة من البلدان.

كما لا تطول الجرائم السيبرانية الأفراد فقط، بل أصبحت جرائم شاملة قد تأخذ شكل هجمات منسقة أو أنشطة إرهابية تطول البنية الأساسية الحساسة للمعلومات للدول.[1]

2- جريمة ناعمة سهلة الإرتكاب:

لا تتطلب الجريمة السيبرانية عنفا أو مجهودا كبيرا في إرتكابها، حيث أنها تتطلب نوعا من الدراية الذهنية و التفكير المدروس القائم على معرفة بتقنية الحاسب الآلي و شبكة الإنترنت على عكس التقليدية التي تتطلب مجهودا عضليا يصل إلى ممارسة العنف و الإيذاء كالضرب أو القتل أو كسر الأبواب.[2]

3- السرعة في تنفيذها:

من صفات الجرائم السيبرانية السرعة التي تتم بها، إذ قد تحدث الأضرار حتى قبل أن تعي الضحية بإستهدافها، و هو قد لا يتيح للضحية الدفاع عن نفسها، و هذا راجع إلى إستخدام الضحايا للإنترنت مدة زمنية طويلة مع ولوجهم إلى مواقع مختلفة محفوفة بالأخطار.[3]

4- ترتكب من خلال الوسائل التقنية:

نظرا للطبيعة الخاصة لهذه الجريمة فإنها ترتكب في بيئة إلكترونية، يستلزم التعامل معها إستعانة الجاني لوسائل وأجهزة تقنية، كالحاسب لآلي بالإضافة أنها ترتكب عبر شبكة الإنترنت، إذ تعتبر هذه الأدوات أساسية لإرتكاب هذه الجريمة.[4]

5- جريمة يصعب إكتشفها:

من خصاص الجريمة السيبرانية أنها من الجرائم التي لا تترك أثرا لملاحظتها و متابعتها، حيث يعمد الجاني إلى إستخدام تقنيات تعرقل الوصول إليه أو معرف التقنية التي إرتكبها للجريمة، كما أن الضحية لا

[1] - ساري محمد الخالد، اتجاهات في أمن المعلومات وأمنها، العبيكان للنشر و التوزيع، الرياض، الطبعة الأولى، 2018، ص 41.
[2] - رفد عيادة الهاشمي، الارهاب الالكتروني، دار أمجد للنشر والتوزيع، عمان، 2019، ص 51.
[3] - ساري محمد الخالد، المرجع السابق، ص 39.
[4] - ميرفت محمد حبايبة، المرجع السابق، ص 43.

يكتشفها مباشرة و لا يشعر بها إما لضعف قدرته الفنية مقارنة بالقدرات الفنية للجاني و مهاراته، أو لعدم رغبة المجني عليه بالتبليغ عن وقوع الجريمة حفاضا على سمعته و ذلك لعدم فقدان الثقة فيه، حيث تلجأ معظم الشركات الكبرى و المصانع و المؤسسات و الجمعيات و البنوك و الجامعات ذات السمعة المرموقة إلى التستر و عدم الإبلاغ على هذه الجرائم، و تفضيلهم حلها تقنيا من خلال موظفي تكنولوجيا المعلومات لديهم.[1]

6- جريمة يصعب إثباتها:

الجريمة السيبرانية تقع في الفضاء السيبراني و الأدلة التي تخلفها تكون أدلة إلكترونية حيث يستطيع المجرم الإلكتروني التخلص من الآثار المادية لجريمته بفضل التقنيات و المهارات المستعملة، حيث يستخدم المجرم غالبا تقنيات إخفاء الهوية والتشويش، و تتم عن طريق نبضات إلكترونية عابرة للدول بواسطة شبكات التواصل و هذا بدوره يجعل التحري عن الأدلة الرقمية و الإلكترونية صعبا للغاية. [2]

7- جريمة مكلفة للضحايا:

يحمل إنتشار الجريمة السيبرانية في طياته تكاليف و خسائر مالية كبيرة سواء أكان ذلك بصفة مباشرة أو غير مباشرة، وتتجسد التكاليف المباشرة وغير المباشرة في الأموال المسحوبة من حسابات الضحية، أو الوقت والجهد المستغرق لإصلاح نظم الحاسوب، بالإضافة إلى التكاليف أعمال صيانة للنظم الحاسوبية.

وتتمثل النفقات غير المباشرة في المقابل النقدي للخسائر التي يتكبدها المجتمع نتيجة وجود ظاهرة جرمية سيبرانية بشكل عام. ويتمخض عن ذلك فقدان الثقة في الخدمات عبر الإنترنت وإنخفاض إقبال الأفراد على الخدمات الإلكترونية. فالتكلفة الإجمالية التي يتحملها المجتمع نتيجة الجريمة السيبرانية قد تتضمن أيضا "تكاليف الدفاع".[3]

الفرع الثاني/ صور الجريمة السيبرانية

تشمل الجريمة السيبرانية طائفة واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوي الحاسوبي، فضلا عن الأعمال التي تمس بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها، و فيما يلي مجموعة من الجرائم السيبرانية و التي تم إعدادها من قبل الأمم المتحدة اللجنة الإقتصادية و الإجتماعية لغربي آسيا "الإسكوا unescwa" من طرف إدارة تكنولوجيا المعلومات و الإتصالات التابعة لها تحت عنوان" إرشادات الإسكوا للتشريعات السيبرانية" و هو مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية:

[1] - ميرفت محمد حبايبة، المرجع السابق، ص 45.
[2] محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية للصحافة و النشر، الطبعة الأولى، 2010، ص42.
[3] - مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دراسة شاملة عن الجريمة السيبرانية، الأمم المتحدة، نيويورك، 2013، ص 41.

1- جرائم التعدي على البيانات المعلوماتية وتشمل كل من:

- جرم التعرض (تعديل أو إلغاء أو محو أو إفساد أو تدمير) للبيانات المعلوماتية.
- جرم إعتراض بيانات معلوماتية.

2- جرائم التعدي على الأنظمة المعلوماتية و تشمل كل من:

- جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه.
- جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية.
- جرم إعاقة عمل نظام معلوماتي.

3- إساءة إستعمال الأجهزة أو البرامج المعلوماتية.

4- جرائم التعدي على الأموال والمعاملات و تشمل كل من:

- جرم الإحتيال أو الغش بوسيلة معلوماتية.[1]
- جرم التزوير المعلوماتي.
- جرم الإختلاس أو سرقة أموال بوسيلة معلوماتية
- جرم أعمال التسويق والترويج غير المرغوب بها.
- جرم الإستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والإستخدام غير المشروع لها.
- جرم الإطلاع على معلومات سرية أو حساسة أو إفشائها.

5- جرائم الإستغلال الجنسي للقاصرين و تشمل كل من:

- جرم إنتاج مواد إباحية لقاصرين بقصد بثها بواسطة نظام معلوماتي.
- جرم عرض مواد إباحية لقاصرين بواسطة نظام معلوماتي.
- جرم توزيع أو بث أو نقل مواد إباحية لقاصرين بواسطة نظام معلوماتي.
- جرم التزود أو تزويد الغير بمواد إباحية لقاصرين بواسطة نظام معلوماتي.
- جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي.
- جرم تحريض القاصرين على أنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية.
- جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية.[2]

6- جرائم التعدي على الملكية الفكرية للأعمال الرقمية و تشمل كل من:

- جرم وضع إسم مختلس على عمل.
- جرم تقليد إمضاء المؤلف أو ختمه.
- جرم تقليد عمل رقمي أو قرصنة البرمجيات.

---

[1] - الأمم المتحدة اللجنة الإقتصادية و الإجتماعية لغربي آسيا، إرشادات الإسكوا للتشريعات السيبرانية، بيروت، 2012، ص133.

[2] - المرجع نفسه، ص134

- جرم بيع أو عرض عمل مقلد أو وضعه في التداول.
- جرم الإعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

7- جرائم البطاقات المصرفية والنقود الإلكترونية و تشمل كل من:

- جرم تقليد بطاقة مصرفية.
- جرم إستعمال بطاقة مصرفية مقلدة.[1]
- جرم قبول الإيفاء ببطاقة مصرفية مقلدة.
- جرم تزوير النقود الإلكترونية.

8- الجرائم التي تمس المعلومات الشخصية و تشمل كل من:

- جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص.
- جرم معالجة معلومات ذات طابع شخصي دون إحترام القواعد القانونية.
- جرم إفشاء معلومات ذات طابع شخصي.
- جرم عدم الإستجابة لطلب الشخص المعني بالإطلاع أو التصحيح.

9- جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية و تشمل كل من:

- جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية.
- جرم تهديد أشخاص أو التعدي عليهم بسبب إنتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية.[2]
- جرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.
- المساعدة أو التحريض بوسيلة إلكترونية على إرتكاب جرائم ضد الإنسانية.

10- جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية و تشمل كل من:

- جرم تملك وإدارة مشروع مقامرة على الإنترنت.
- جرم تسهيل وتشجيع مشروع مقامرة على الإنترنت.
- جرم ترويج الكحول للقاصرين على الإنترنت.
- جرم ترويج المواد المخدرة على الإنترنت.

11- جرائم المعلوماتية ضد الدولة والسلامة العامة و تشمل كل من:

- جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية.
- جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية.
- جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة.
- جرم العبث بالأدلة القضائية المعلوماتية.[3]

---

[1] - الأمم المتحدة اللجنة الإقتصادية و الإجتماعية لغربي آسيا، المرجع السابق، ص 135.

[2] - المرجع نفسه، نفس الصفحة..

[3] - نفس المرجع، ص 136.

- جرم بث بيانات تهدد الأمن والسالمة العامة بوسيلة معلوماتية.
- جرم الإرهاب بوسيلة معلوماتية.
- جرم التحريض على القتل بوسيلة معلوماتية.[1]
- التجسس الإليكتروني و الحرب الإلكترونية.

12- **جرائم تشفير المعلومات** و تشمل كل من:

- جرم عدم حيازة ترخيص أو تصريح عن تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير.
- جرم تقدمي وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص.
- جرم بيع أو تأجير وسائل تشفير ممنوعة.[2]

لقد أعدت الإسكوا هذه الإرشادات ليستعين بها المشرعون عند صياغة التشريعات السيبرانية، وليستفيد منها أصحاب القرار في الوزارات والمؤسسات الحكومية من أجل وضع قوانين جديدة أو تعديل القوانين النافذة، وليعتمد عليها القضاة والمحامون في معاجلة المسائل القانونية المتعلقة بالفضاء السيبراني. كما يستفيد من هذه الإرشادات أيضاً الأكاديميون والباحثون والطلاب المهتمون بتنظيم الفضاء السيبراني، وكذلك الأفراد الذين يأملون بأن يصبح الفضاء السيبراني فضاء آمناً وموثوقا.[3]

الفرع الثالث/ أركان الجريمة السيبرانية:

تقوم الجريمة السيبرانية بتوافر أركانها و التي تتلخص في:

1- الركن المفترض:

هو وجود جهاز إلكتروني وفي الغالب يكون جهاز الكمبيوتر كركن مفترض يشكل الوسيلة المستخدمة لإرتكاب السلوك الإجرامي للركن المادي في البيئة الرقمية المتصلة بالإنترنت.[4]

2- الركن المادي:

يتكون الركن المادي للجرائم السيبرانية من السلوك الإجرامي المتمثل في النشاط التقني والأفعال غير مشروعة في مجال الحاسوب والإنترنت، و يتخذ الركن المادي عدة صور بحسب كل جريمة، كقيام الجاني بتجهيز الحاسوب ليحقق الجريمة، و من ذلك تحميل الحاسوب ببرمجيات إختراق أو أن يقوم بإعدادها، و كذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها علي الجهاز المضيف Hosting Server، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.[5]

---

[1] - الأمم المتحدة اللجنة الإقتصادية و الإجتماعية لغربي آسيا، المرجع السابق، ص 136.
[2] - المرجع نفسه، ص 137.
[3] - نفس المرجع، ص أ.
[4] - هيثم عبد الرحمان البقلي، الجرائم الإلكترونية الواقعة على العرض: بين الشريعة والقانون المقارن، دار العلوم للنشر والتوزيع، 2010، ص 21.
[5] - علي جبار صالح الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، 2018، ص 74.

كما يعد من قبيل الركن المادي الإستعمال السيء لكل الأجهزة الإلكترونية ما من شأنه الإضرار بالغير سواء أفراد أو شركات أو مؤسسات عامة أو خاصة.

أما النتيجة فتتمثل في تحقق الجريمة بناء على السلوك الإجرامي، كالقرصنة أو الإختراق أو إتلاف البيانات و تزوير المعلومات و ما شابهه و التدخل في خصوصيات الغير دون وجه مشروع.

أما بالنسبة للعلاقة السببية فتثير إشكالا كون أن من خصائص الجرائم السيبرانية أنها صعبة الإكتشاف وصعبة الإثبات و ذات طابع دولي عابر للقارات، فكل هذا يصعب من تطبيق نظريات فقهاء القانون المتعلقة بالعلاقة السببية في الجريمة السيبرانية خلافا للجريمة العادية سواء النظرية السببية الملائمة أو نظرية تعدد الأسباب و السبب و ذلك لصعوبة القبض على الجاني و صعوبة إكتشاف الدليل الجنائي الرقمي.[1]

3- الركن المعنوي:

يتمثل الركن المعنوي في الجرائم السيبرانية في القصد الجنائي العام المتمثل في عنصري العلم و الإرادة مثل: الإدخال العمدي لبرنامج معلوماتي أو نشر الفيروسات على الشبكة المعلوماتية أو نظام معلوماتي إلكتروني، أو أي فعل عمدي آخر كإغراق أو تعطيل أو إتلاف محتويات أو إيقاف موقع إلكتروني ما عن العمل، أو جريمة الدخول بدون تصريح إلى نظام معلوماتي إلكتروني بقصد الحصول أو إتلاف بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية، تجارية أو إقتصادية، أو جريمة التحايل على العنوان البروتوكولي للإنترنت بقصد إرتكاب جريمة أو الحيلولة دون إكتشافها كالدخول و البقاء غير المشروع في نظام إلكتروني.[2]

كما تتطلب طائفة من الجرائم لقيامها توافر القصد الجنائي الخاص الذي يقوم على أساس غاية معينة أو مسار بعيد تسلكه إرادة الجاني مما هو عليه في القصد الجنائي العام القائم على عنصري "العلم و الإرادة " ومن ذلك مثلا جريمة نشر الفيروسات، كأن يكون الباعث على الجريمة هو الإنتقام أو الكراهية أو الحقد أو الحصول على مكاسب مادية.[3]

كما إتجهت السياسة الجنائية الحديثة إلى تجريم الإعتداء **غير العمدي** على المصالح محل الحماية الجناية في نطاق بيئة الأنظمة الإلكترونية و السبب في ذلك أن هناك بعض الحالات التي يدخل فيها مرتكب الفعل إلى الأنظمة بغرض الترفيه، و مع ذلك ينتج عنها أضرار خطيرة تلحق بأنظمة المعلومات خاصة ما يتعلق بالأمن القومي أو مصلحة الدولة الإقتصادية أو علاقاتها الدولية و الإقليمية، رغم أن نية الجاني فيها لا تتجه إلى الإتلاف أو إعاقة النظام.[4]

---

[1] - عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون و الإقتصاد، الرياض، الطبعة الأولى، 2012، ص 94.
[2] - حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، دار الفكر والقانون للنشر و التوزيع، 2015، ص 37-38.
[3] - المرجع نفسه، ص 39.
[4] - نفس المرجع، ص 40-41.

4- الركن الشرعي:

و هو النص القانوني الذي ينص على تجريم الفعل أو السلوك، حيث تنص القاعدة القانونية على أنه "لا جريمة و لا عقوبة إلا بنص"، إذ أخذت معظم التشريعات الدولية بتجريم الأفعال و السلوكيات المرتبطة بالجرائم السيبرانية في ضل مكافحتها تحت مسميات مختلفة.[1]

و في مستعرض الإستبيان الخاص بالدراسة الشاملة عن الجريمة السيبرانية التي قام بها مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، وجد أن عددا قليل من الدول التي أشارت في تشريعها الوطني أو إستعملت كلمة "جريمة سيبرانية" في عنوان التشريع أو في نطاق الأحكام التشريعية، ومن المسميات الأكثر شيوعا إلى حد ما في التشريعات؛ "جرائم الحاسوب"، "جرائم الإتصالات الإلكترونية"، "جرائم تكنولوجيا المعلومات"، أو "جرائم التكنولوجيا المتقدمة "،"جرائم خاصة بتكنولوجيات المعلومات والاتصال".

فمن الناحية العملية، أصدرت العديد من الدول تشريعات تتضمن جرائم جنائية والتي تم تضمنيها في مفهوم الجريمة السيبرانية، مثل النفاذ غير المشروع إلى نظام حاسوبي، أو التدخل في النظم الحاسوبية أو البيانات الحاسوبية و منها على سبيل المثال: قانون جرائم الحاسوب الماليزي، قانون جرائم الحاسوب السريلانكي، قانون جرائم الحاسوب السوداني، قانون جرائم الإنترنت والحاسوب لبوتسوانا، قانون جرائم الإنترنت لكمبوديا، قانون الجرائم المتعلقة بالشبكات الإلكترونية لجامايكا.[2]

قانون الأمن السيبراني لكل من المملكة المغربية و المملكة الأردنية، قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها الجزائري.

المطلب الثاني :

الطبيعة القانونية للمجرم السيبراني

تحتاج الجرائم السيبرانية في إرتكابها إلى جهد عقلي و تقني من أشخاص ذوي مهارات خاصة لهم القدرة على التعامل مع جهاز الحاسوب بمستوى تقني لإرتكاب الأفعال غير المشروعة، كما يمكن أن تتم الجريمة السيبرانية بتعاون أكثر من شخص على إرتكابها فمنهم من يغطيها تقنيا و فنيا و منهم من يتولى أمور التلاعب و تحويل العائدات المكاسب.

الفرع الأول/ تعريف المجرم السيبراني:

هو مجرم يتمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته التقنية في إختراق الشبكات و كسر الشفرات و كلمات المرور موظفا مهاراته في تخزين البيانات و المعلومات و التحكم في أنظمة الشبكات، و قد أثبتت الدراسات في علم النفس الجنائي أن المجرم السيبراني ليس لديه أي شعور بعدم مشروعية الأفعال التي يمارسها،

[1] - زياد بن محمد عادي العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث أشكالها، خصاصها، أركانها و الدافع من إرتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، عمان، الأردن، المجلد 03، العدد 01، 2020، ص 14.

[2] - مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، المرجع السابق، ص 17.

و عدم إستحقاقهم للعقاب، كما تغيب مشاعر الإحساس بالذنب لديه، كما أنهم في الغالب يتميزون بأنهم أفراد ذوي مكانة في المجتمع من أصحاب الوظائف الحيوية سواء في القطاع العام أو الخاص.[1]

الفرع الثاني/ خصائص الجاني في الجرائم السيبرانية:

يتميز المجرم السيبراني بمجموعة من الخصائص والتي تتمثل في:

1- تمتع الجاني بالذكاء:

يتمتع الجاني في هذه الجرائم بنظرة غير تقليدية له على إعتبار أنه يوصف غالبا بدرجة عالية من الذكاء المعلوماتي، تجعل من الصعب تصنيفه بحسب التصنيف الإجرامي المعتاد، لذا ينظر في تحديد أنواع الجناة في الجرائم الإلكترونية إلى الهدف من إرتكابه لهذه الجرائم كمعيار للتمييز فيما بينهم.[2]

2- مجرم عائد إلى الإجرام:

كثيرا ما يعود مرتكبي الجرام السيبرانية إلى إرتكاب جرائم أخرى في هذا المجال، إنطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم و تقديمهم للمحاكمة في المرة الأولى، مما يؤدي بهم إلى العود للإجرام، مما قد ينتهي بهم المطاف إلى القبض عليهم و تقديمهم للمحاكمة مرة أخرى.[3]

3- مجرم متخصص و محترف:

لا يسهل على الشخص العادي إرتكاب الجرائم السيبرانية إلا إذا كان شخص متخصص في مجال تقنية الكمبيوتر و المعلومات و على درجة عالية من الخبرة و المهارة في إستخدامها، حيث يقتضي الأمر كثير من الدقة و التخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر و المعلوماتية.[4]

الفرع الثالث/ أصناف المجرم السيبراني:

لمرتكبي الجرائم السيبرانية عدة أصناف منها:

1- الهواة: وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه.

2- القراصنة: ومنهم

أ) **الهاكر** (hacker): هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أو اثبات الذات.

---

[1] - فارس محمد العمارات، إبراهيم الحمامصة، الأمن السيبراني -المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، الطبعة الاولى، 2022، ص 81.

[2] - عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمان، المحكمة الرقمية و الجريمة المعلوماتية، مكتبة القانون و الإقتصاد، الرياض، الطبعة الأولى، 2012، ص 52.

[3] - غادة نصار، الإرهاب و الجريمة الالكترونية، العربي للنشر والتوزيع، القاهرة، 2017، ص 44.

[4] - المرجع نفسه، ص 44-45.

ب) **الكراكرز (crackers):** وهم من يقومون بالتسلل إلى أنظمة المعالجة للاطلاع على المعلومات المخزنة و إلحاق الضرر إما بالسرقة أو العبث بها، كما يتابعون عن كثب آخر الأخبار و برامج الحماية للأجهزة و المعلومات، الى حد أنهم ينشؤون النوادي لتبادل المعلومات.[1]

ج) **القراصنة الخبثاء أو المؤذين (Malicious hacker):** هدفهم إلحاق الخسائر بالمجني عليهم وليس الحصول على مكاسب مادية، و يعتبر من أشخاص هذه الطائفة مخترعو الفيروسات و موزعوها.[2]

3- الجماعات الإرهابية أو المتطرفة:

و هم جماعة تعمل تحت معتقدات و أفكار سياسية، إجتماعية أو دينية، بغرض فرض معتقداتهم باللجوء إلى النشاط الإجرامي، عن طريق إنشاء مواقع إلكترونية خاصة و إختراق الشبكات و أنظمة الحاسبات الآلية و التي تم الإعتماد عليها في تسيير النشاطات في مختلف المؤسسات و الدول.

4- الجماعات المنظمة:

وهدفهم من إرتكاب الجرائم السيبرانية تحقيق ربح مادي بطريقة غير مشروعة، و هم مجموعات يعملون بطريقة منظمة فينطبق على أفعالهم وصف الجريمة المنظمة. إذ يشترك في تنفيذ النشاط الإجرامي أكثر من شخص. [3]

5- جواسيس الصناعة:

تعتبر هذه الفئة أحيانا فئة فرعية من الجماعة الإجرامية، وأهدافها محددة بالحصول على الأسرار التجارية، أو الابتزاز لأسباب تتعلق بالمصلحة الاقتصادية، أو تخريب المنافسة، وغالبا ما تشاهد في عالم الشركات.[4]

الفرع الرابع/ دوافع إرتكاب الجرائم السيبرانية:

تتعدد الأسباب التي تدفع بالمجرم السيبراني لإرتكاب الجرائم السيبرانية و منها:

1- تحقيق أرباح ومكاسب مادية:

يعد الباعث المادي على إرتكاب الجرائم السيبرانية من أهم الدوافع التي تحفز المجرم السيبراني على إقترافها، وذلك لما تحققه من عوائد مادية طائلة، إذ أن من خصائص الجرائم السيبرانية سرعة التنفيذ و صعوبة إكتشافها و ذلك خلافا للجرائم التقليدي.[5]

---

[1] - فارس محمد العمارات، إبراهيم الحمامصة، المرجع السابق، ص 81.

[2] - محمد علي سكيكر، المرجع السابق، ص 54.

[3] - المرجع نفسه، ص 55.

[4] - خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكولاي لوزينسكي، الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، الأمم المتحد ة، جنيف ،2021، ص 14.

[5] - محمد مصطفى رفعت، الرأي العام في الواقع الافتراضي وقوة التعبئة الافتراضية، العربي للنشر والتوزيع، القاهرة، الطبعة الأولى، 2018، ص 229.

2- قهر النظام وإثبات التفوق على تطور الوسائل التقنية:

في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الأمنية للأنظمة الإلكترونية واختراقها ليثبت براعته في القدرة على تحدي أي تطور جديد في عامل التقنية والتكنولوجيا. ويرتفع مؤشر الزيادة لدى فئات صغار السن من مرتكبي هذه الجرائم.[1]

3- دافع التعلم:

يعتبر حب التعلم و الإستطلاع من الأسباب الرئيسة التي تدفع لإرتكاب مثل هذه الجرائم لأن المخترق يعتقد بأنه يحق للجميع التعرف و الإستفادة من المعلومات المتواجدة على أجهز الحاسوب و الأنظمة و أن لا تبقى حكرا على أحد لدى يسعى لجمع المعلومات و تعلمها وكثيراً ما نجد أن قراصنة الأنظمة يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب الالكترونية هو التعلم فقط فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولو بطرق غير مشروعة.[2]

4- دافع سياسي أو عقائدي:

يتم من خلال المجرمين المعادين للحكومات، و ذلك عبر تخريب المواقع الحكومية أو إختراق الحسابات الحكومية عبر منصات التواصل الإجتماعي مثل **تويتر** و **فيسبوك** لنشر أخبار و معلومات غير صحيحة بغرض إثارة الفتنة في الرأي العام.

5- دافع الإنتقام:

و هي من أخطر الدوافع التي يقوم بها المجرم السيبراني، و ذلك من خلال الثأر من الأشخاص لأسباب شخصية كإنتقام الموظف الذي تم فصله من المنشأة التي كان يعمل بها فيقوم بإختراق نظامها تشفيا و إنتقاما لنفسه مما يحدث أضرارا بالمنشأة.[3]

6- التسلية و اللهو:

عدد غير قليل من مخترقي الأنظمة يعتبرون أن عملهم هذا وسيلة للمرح و التسلية و تمضية أكبر وقت ممكن في أنظمة و حواسيب الآخرين، ويكون هذا الإختراق غالبا سلميا و دون أن يحدث تأثير يذكر.[4]

---

[1] - مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الأمانة العامة، سلطنة عمان، 2016، ص 29.

[2] - بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2014، ص 69.

[3] - زياد بن محمد عادي العتيبي، المرجع السابق، ص 15.

[4] - بشرى حسين الحمداني، المرجع السابق، ص 70.

الخلاصة:

أدى التطور المستمر في تكنولوجيا المعلومات و الإتصالات إلى ظهور البنية التحتية الرقمية و هو مجال عالمي يتكون من الشبكات المترابطة لتكنولوجيا المعلومات والبيانات وشبكات الاتصال وأنظمة الحاسوب والمعالجات أو بما يعرف بالفضاء السيبراني فهو مجال يستحضر فيه الأفراد و الشركات و الدول و الحكومات مصالحهم و إهتماماتهم المختلفة ، وأصبح الفضاء السيبراني أحد سمات المجتمع الحديث، وهو ما يعمل على تعزيز وتمكين الإتصال السريع بين أنظمة القيادة والتحكم الموزعة بشكل كبير، وتخزين ونقل المعلومات و البيانات بكميات هائلة. وسارت كل هذه الأشياء الآن من المسائل المسلم بها لدى المجتمع وأصبحت عاملاً أساسيًا للأعمال التجارية، و تقديم الخدمات في حياتنا اليومية. ويمكن رؤية إنتشار الفضاء السيبراني في كل مكان والإعتماد عليه حتى في الميادين العسكرية، إذ يعد فضاء عالمي لا يرتبط بأي نطاق محدد جغرافيا.

و مع هذا التطور للفضاء السيبراني كبيئة تفاعلية رقمية ظهر الأمن السيبراني كحتمية إلزامية يهتم بممارسة حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات و الجرائم الرقمية والتي تستهدف عادة الوصول للمعلومات الحساسة، أو تغييرها، أو إتلافها، و إبتزاز المال من المستخدمين، وتعطيل العمليات التجارية، و يأتي الإهتمام المتزايد للأمن السيبراني مع زيادة الجرائم السيبرانية و تطورها المستمر.

حيث تباينت تسمية الجرائم عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة إستخدام الكمبيوتر، مرورا بإصطلاح إحتيال الكمبيوتر، والجريمة المعلوماتية، فإصطلاحات جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الإنترنت، إلى آخر المصطلحات و هو الجرائم السيبرانية.

فالجريمة السيبرانية جريمة مستحدثة، مرتبطة أساسا بوجود نظام معلوماتي، وترتكب من مجرم متميز ذي دراية كافية بطريقة عمل هذا النّظام وإستغلاله في القيام بأعمال غير مشروعة، وهذه الجرائم إما أن يكون محلها المال، وإما أن يكون محلها الأشخاص واما أن يكون محلها الحقوق الذهنية كحق المؤلّف، ولما لذلك من خطورة قصوى قد تؤدي للإنهيار إقتصادي كما حدث في عدد من الدول بسبب عمليات القرصنة المنظمة على بنيتها السيبرانية أو الإنهيار الأمني بمعناه السياسي، كما يمكن أن تؤدي تلك التداعيات إلى إنهيار أخلاقي وإجتماعي.

فالإنتشار الرهيب للجرائم السيبرانية في الفضاء السيبراني دفع بالكثير من الدول بإعتبارها فاعل دولي في الفضاء الإفتراضي لبدل المجهودات لمجابهة هذه التحديات و هذا ما سنتطرق إليه في الفصل الثاني تحت عنوان آليات مكافحة الجرائم السيبرانية.

الفصل الثاني:

آليات مكافحة الجرائم السيبرانية

الفصل الثاني:

آليات مكافحة الجرائم السيبرانية

أدت التطورات المتتالية في علوم الحاسب الآلي وتقنية المعلومات وشبكة الإنترنت إلى نقلة علمية وتطبيقية حضارية إيجابية هائلة في كافة مجالات الحياة ، ومع انتشار استخدام الانترنت والشبكات المعلوماتية ، وتزايد استخدام الأفراد لها ، أصبح هناك في المقابل تزايد كبير أيضا في نسبة الجريمة السيبرانية القائمة على الشبكات المعلوماتية بأنواعها المختلقة ، عن طريق أفراد و منظمات إجرامية متخصصة في إرتكاب كافة الجرائم الإلكترونية ، وإدراكا من المجتمع الدولي لمدى الحاجة الماسة لتعاون دولي وإقليمي فعال يكبح جماح الجريمة الإلكترونية ويحد من مخاطرها الاقتصادية والاجتماعية والأمنية بعد الارتفاع الكبير في عدد ضحايا مستخدمي شبكة الإنترنت حول العالم، الأمر الذي يستوجب معه تضافر كافة الجهود الدولية والإقليمية والوطنية بغرض التصدي لتلك الجرائم المستحدثة لخطورتها الشديدة وصعوبة إثباتها.

وعليه سوف نتناول في هذا الفصل آليات مكافحة الجرائم السيبرانية فيما يلي:

المبحث الأول: آليات مكافحة الجرائم السيبرانية على الصعيد الدولي، أما في المبحث الثاني سنتناول آليات مكافحة الجرائم السيبرانية على الصعيد الوطني.

المبحث الأول:

آليات مكافحة الجرائم السيبرانية على الصعيد الدولي

تعتبر الجرائم السيبرانية من أخطر الجرائم التي يشهدها العالم اليوم، والتي تشكل الوجه السلبي لإنتشار استعمال تكنولوجيات العالم والاتصال والانتقال من العالم التقليدي إلى العالم الرقمي الذي يقوم على اقحام التكنولوجيا في جميع مجالات الحياة، ومع الإنتسار الهائل لهذه الجرائم فقد اصبحت تشكل تهديدا ليس فقط للأفراد، بل للدول ومؤسساتها، و الهيئات العمومية والخاصة وتعدى ذلك أيضا إلى تهديد استقرار الدول وأمنها، الأمر الذي جعل العمل على حماية الفضاء السيبراني من مخاطر الجرائم السيبرانية والوقاية منها يتزايد كل يوم ويفرض على الدول تسخير كافة الوسائل القانونية و المادية التي من شأنها المساهمة في الوقاية من مخاطر الجرائم السيبرانية بمختلف أشكالها و مكافحتها، بما يحول دون انتشارها و تطورها بصورة أكبر مما عليه اليوم.

المطلب الأول:

الجهود الدولية و الإقليمية لمكافحة الجرائم السيبرانية

أدى إنتشار التكنولوجيا و تقنيات المعلومات وكذا الجرائم المرتبطة بها إلى إهتمام الدول والمنظمات الدولية ببذل وتكثيف الجهود الرامية لمواجهة ومجابهة الخطورة التي يشكلها هذا الإجرام المستحدث لا سيما وأنه من الجرائم العابرة للحدود، وفيما يلي سوف نستعرض أهم الجهود الدولية سواء تمثل ذلك في قرارات المنظمات الدولية أوعن طريق الإتفاقيات الدولية بشأن الجرائم السيبرانية و ذلك لتحقيق الأمن السيبراني و لضمان سلامة المؤسسات و الأفراد في مواجهة المخاطر السيبرانية.

الفرع الأول/ جهود المنظمات و الهيئات الدولية:

إنعكس الإهتمام العالمي في مكافحة الجرائم السيبرانية في العديد من المؤتمرات و المبادرات الدولية الهادفة إلى تعزيز الأمن السيبراني العالمي ومن بين هذه الجهود و المبادرات ما يلي:

1- جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية:

قدمت الأمم المتحدة جهودًا قيمة من أجل مواجهة ومجابهة الجريمة السيبرانية، مؤكدة على وجوب تضافر الجهود الدولية والعمل المشترك بهدف الحد من إنتشار هذا النوع من الجرائم، ومن أهم المؤتمرات التي عقدتها الأمم المتحدة بهذا الشأن على سبيل المثال:

أ) المؤتمر السابع لمنع الجريمة ومعاملة المجرمين:

عقد المؤتمر في مدينه ميلانو الإيطالية في الفترة الممتدة من 26 أوت إلى 06 سبتمبر 1985 وحينها كلفت لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالج الآلية و الإعتداء على الحاسب الآلي و إعداد تقرير قصد عرضه على المؤتمر الثامن.

ب) المؤتمر الثامن للأمم المتحدة:

عقد في هافانا الكوبية في الفترة الممتدة من 27 أوت الى 07 سبتمبر 1990 والذي أقر المعاهدات النموذجية لتسليم المجرمين وتبادل المساعدة في المسائل الجنائية ونقل الإجراءات في المسائل الجنائية ونقل والإشراف على المجرمين المحكومين عليهم بأحكام مشروطة أو المفرج عنهم إفراجا مشروطا[1].

[1]- أمال بيدي، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، جامعة تيارت، المجلد 08، العدد 01، 2022، ص 306.

أما في مجال الجرائم المتعلق بالحاسوب فلقد أشار قرار هذا المؤتمر إلى أن هناك إجراءات يستوجب على الدول إتخاذها والتي من بينها:

- تحديث القوانين وأغراضها الجنائية من أجل تطبيق أفضل القوانين الجنائية الراهنة وعلى نحو ملائم وإدخال تعديلات إن تطلب الأمر ذلك.
- مصادرة العائد والأصول من الأنشطة غير المشروعة.
- إتخاذ تدابير الأمن والوقاية مع مراعاة خصوصية الأفراد و إحترام حقوق الإنسان.
- رفع الوعي لدى الجماهير و القضاة و الأجهزة المعنية والتأكيد على أهمية مكافحة هذا النوع من الجرائم ومحاكمة مرتكبها.
- حماية مصالح وحقوق ضحايا جرائم الحاسوب[1].

ج) المؤتمر التاسع للأمم المتحدة حول منع الجريمة ومعاملة المجرمين:

تم عقده بالقاهرة المصرية في الفترة الممتدة بين 28 أفريل و05 ماي 1995، أوصى هذا المؤتمر بوجوب حماية الإنسان في حياته الخاصة و ملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين افراد المجتمع الدولي لإتخاذ الإجراءات الضرورية و المناسبة[2].

د) المؤتمر الثاني عشر للأمم المتحدة حول منع الجريمة والعدالة الجنائية:

إنعقد المؤتمر في السلفادور البرازيلية في الفترة من 12 و19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء بتعمق مختلف تطورات في مجال مكافحة الجريمة لاسيما أن منظمة الأمم المتحدة تعد الإطار الأمثل لمكافحة الإجرام السيبراني وقد وضعت مجموعه من القواعد الموضوعية والإجرائية لمواجهة هذا النوع من الجرائم.

وتأكيدا منها في هذا المؤتمر جاء البند 41 من تقريره بحث الدول على بناء قدرات سلطاتها الوطنية من أجل التعامل مع الجرائم الإلكترونية، بما في ذلك المنع والكشف و التحقيق وملاحقة هذه الجريمة بكافة أشكالها وتعزيز الأمن في شبكات الكمبيوتر[3].

هـ) المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية:

إنعقد في الدوحة بقطر في الفترة الممتدة بين 12 و19 أفريل 2015، و من أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة السيبرانية ما يلي:

[1] - أمال بيدي، المرجع السابق، ص 307.
[2] - المرجع نفسه، ص 308.
[3] - نفس المرجع، ص 308 -309.

– وجوب إستحداث أدوات وبرامج من أجل تسهيل مكافحه الجريمة السيبرانية ومنعها.

– بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية و التحقق فيها، وعملية الإستدلال الجنائي الرقمي وكيفية التعامل مع الأدلة الإلكترونية.

– التأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة السيبرانية[1].

و) قرارات الجمعية العامة للأمم المتحدة:

– القرار (121/45) لعام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.[2]

– القرار رقم (63/55) المؤرخ في 2000/12/04، والقرار رقم (121/56) المؤرخ في 2001/12/19 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عقد وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.[3]

– القرار رقم (239/57) المؤرخ في 2003/01/31، والقرار رقم (199/58) المؤرخ في 2004/01/30 بشأن «إنشاء ثقافة عالمية للأمن السيبراني» ودعوة الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.[4]

– قرار رقم (247/74) المؤرخ في 27 ديسمبر 2019 بشأن مكافحة إستخدام تكنولوجيا المعلومات والإتصال للأغراض الإجرامية. إذ يدعو هذا القرار إلى ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة استخدام تكنولوجيا المعلومات والإتصالات للأغراض الإجرامية، من خلال تقديم المساعدة التقنية إلى البلدان النامية بناء على طلبها من أجل تحسين التشريعات وأطر العمل الوطنية وبناء قدرات السلطات الوطنية بغية التصدي لذلك الإستحدام بكل أشكاله، بما يشمل منعه والكشف عنه والتحقيق فيه وملاحقة مرتكبيه قضائيا.[5]

2– الإتحاد الدولي للإتصالات:

يعمل الإتحاد على مساعدة الحكومات في الإتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للإتصالات، وقد وضع الإتحاد الدولي للإتصالات مخططا لتعزيز الأمن السيبراني العالمي يتضمن تحقيق سبعة أهداف هي:

---

[1]- أمال بيدي المرجع السابق، ص 309.

[2] - فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق و الحريات، جامعة محمد خيضر بسكرة، المجلد 03، العدد 02، 2015، ص 11.

[3] - المرجع نفسه، نفس الصفحة.

[4]- نفس المرجع، نفس الصفحة.

5 - الجمعية العامة للأمم المتحدة، قرارات الدورة 74، قرار رقم (247/74) المؤرخ في 27 ديسمبر 2019، البند رقم 107.

- وضع إستراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.
- وضع إستراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكلي التنظيمية والسياسات المتعلقة بجرائم الإنترنت.
- وضع إستراتيجية لتحديد الحد الأدنى المقبول عالميا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- وضع إستراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.
- تطوير إستراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.
- تقديم المشورة بشأن إمكانية إعتماد إطار إستراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها.[1]

3- منظمة التعاون الاقتصادي والتنمية:

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي و تناغم التطور الإقتصادي مع التنمية الإجتماعية، بدأت هذه المنظمة الإهتمام بالجريمة السيبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة و قواعد إرشادية تتصل بتقنية المعلومات، و يعد الدليل المتعلق بحماية الخصوصية و قواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها.
فأصدرت في سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة و المقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من أفعال سوء استخدام الحاسوب و التي على الدول تجريمها.[2]
و في عام 1992 و ضعت المنظمة توصيات و إرشادات خاصة بأنظمة المعلومات و أوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة تتمثل في فرض قيود على تجميع البيانات، كما تنص على أن تتعلق البيانات بالغاية و الغرض الذي سوف تستخدم من أجله، إذ يقتضي الإلتزام بعدم إفشاء البيانات الشخصية و نشرها لغير المصرح لهم بذلك، كما يمكن محاسبة المصرح لهم في حالة تجاوز الإجراءات التي تكفل حماية البيانات الخاصة .[3]

1 - عقل يوسف مقابلة، مواجهة الإرهاب السيبراني في القانون الجزائي الأردني والمعاهدات الدولية ، المجلة الدولية للدراسات القانونية والفقهية المقارنة، الأردن، المجلد 01، العدد 03، 2020، ص 116.
2 - مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث و الدراسات، جامعة غرداية، المجلد 12، العدد 02، 2019، ص 709.
3 - المرجع نفسه، ص 710.

4- اللجنة الاقتصادية والاجتماعية لدول غرب آسيا (الإسكوا):

تأسست لجنة الأمم المتحدة الاقتصادية والاجتماعية لغربي آسيا (يونسكوا أو الإسكوا) عام 1973، وقد أسسها المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة بقرار (LV 1818) كبديل لمكتب الأمم المتحدة الاقتصادي والاجتماعي في بيروت (يونيسوب)، ويعتبر الأمن السيبراني من بين القضايا التي تعالجها اللجنة ضمن تقاريرها ومؤتمراتها والأبحاث والدراسات التي تشرف عليها، ومن بين جهود اللجنة ما يلي:

في سنة 2014 عقدة اللجنة ورشة عمل في مسقط بعمان بالتعاون مع المركز الإقليمي للأمن السيبراني للإتحاد الدولي للإتصالات، حيث كانت الورشة تهدف إلى بناء القدرات الوطنية في المنطقة العربية لتعزيز الأمن السيبراني و مواجهة الجرائم السيبرانية، كما إستضافت اللجنة في سنة 2018 حوارا إقليميا و إجتماعا للخبراء بشأن حوكمة الإنترنت و الأمن السيبراني تمحور حول تعزيز الثقة و السلامة و الأمن في الفضاء السيبراني.[1]

5- المنظمة العالمية للملكية الفكرية:

إهتمت هذه المنظمة بالمجال السيبراني وذلك بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، حيث تم الإنفاق على توفير الحماية لهما بواسطة الإتفاقيات الدولية خاصة "إتفاقية التريبس" و "إتفاقية برن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها وخاصة تشريعات حق المؤلف، و كذا وضع عقوبات على كل أعمال تزوير في العلامات التجارية و القرصنة المتعمدة و المركبة في إطار تجاري.[2]

الفرع الثاني/ أهم الإتفاقيات والمعاهدات الدولية المتعلقة بمكافحة الجرائم السيبرانية:

إهتم المجتمع الدولي بموضوع مكافحة الجرائم السيبرانية إدراكا منه لمدى خطورة هذه الجرائم، حيث وقعت العديد من الإتفاقيات والمعاهدات وذلك لتعزيز التعاون من أجل الحد منها، وعليه سنتطرق لأهمها فيما يلي:

1- الإتفاقية الأوروبية المتعلقة بحماية الأفراد عند معالجة البيانات الشخصية:

صدرت سنة 1981 عن المجلس الأوروبي "اللجنة الوزارية " وفي عام 1985 صدرت عن المجلس ذاته التوصية رقم (R 20/85) المتعلقة بالبيانات الشخصية في أغراض التسوق المباشر ثم صدر التوجيه الأوربي لسنة 1995 و الخاص بحماية الأشخاص الطبيعيين في مواجهة معالجة البيانات الشخصية وحرية تداول تلك البيانات ثم التوجيه الأوروبي رقم (EC 97/66) لسنة 1997 بشأن معالجة هذه البيانات وحماية الخصوصية في مجال الاتصالات وقد أصبح هذا التوجيه نافذا في 15 اكتوبر 1998 أما في 12 يوليو 2002 فقد أصدر المشرع الأوروبي التوجيه (EC 2002/ 58) و الخاص بمعالجة البيانات ذات الطابع الشخصي و الحياة الخاصة في إطار الانترنت و العمل به[3].

---

[1] - نعيمة حاجي، الجريمة السيبرانية و الجهود الدولية لمكافحتها، مجلة النبراس للدراسات القانونية، جامعة العربي التبسي-تبسة، المجلد 06، العدد 01، 2021، ص 70.

[2] - بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، المجلد 07، العدد 02، 2022، ص 310.

[3] - سامية بساعد، حماية البيانات الشخصية للمستهلك من مخاطر الدفع الالكتروني ، مجلة الحقوق والعلوم الإنسانية، جامعة الشهيد زيان عاشور الجلفة، المجلد 15، العدد 01، 2022، ص 1413.

2- معاهدة الويبو بشأن حق المؤلف لسنة 1996:

أبرمت هذه المعاهدة في عام 1996 ودخلت حيز التنفيذ عام2002 ، وهي عبارة عن إتفاق خاص في إطار" إتفاقية برن " وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وكل طرف متعاقد(حتى وإن لم يكن ملتزما باتفاقية برن) يجب أن يمتثل للأحكام الموضوعية الواردة في وثيقة 1971 (باريس) لإتفاقية برن بشأن حماية المصنفات الأدبية والفنية لسنة 1886. وفضلاً عن الحقوق المنصوص عليها في إتفاقية برن، تمنح هذه المعاهدة بعض الحقوق الاقتصادية للمؤلفين، ومدة الحماية المقررة بموجب هذه المعاهدة 50 سنة على الأقل لأي مصنف، وتتناول المعاهدة أيضا موضوعين يتعين حمايتهما بموجب حق المؤلف وهما:

- برامج الحاسوب، أيا كانت طريقة التعبير عنها أو شكلها.
- مجموعات البيانات أو المواد الأخرى"(قواعد البيانات)"، أيا كان شكلها، إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها.[1]

3- إتفاقية بودابست 2001 لمكافحة الجرائم السيبرانية:

تعد معاهدة بودابست لمكافحة الجرائم السيبرانية (convention on cybercrime) أولى المعاهدات المتعلقة بمكافحة الجرائم السيبرانية والتي تمت في العاصمة المجرية بودابست في 2001/11/23 و التي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت و الاستخدام السيء لها وهي تمثل ركيزة أساسية لمكافحة الجرائم السيبرانية منذ دخولها حيز النفاذ في جويلية 2004. [2]

وقد وقعت على المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان وجنوب إفريقيا، والولايات المتحدة الأمريكية، حيث تتضمن الإتفاقية 48 مادة مقسمة على 04 فصول توفر من خلالها أسس الأمن العام.

إذ تضمنت هذه الاتفاقية مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشؤون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقيات الدولية، إذ تهدف الإتفاقية إلى: [3]

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي،
- الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة.

---

[1] - شريهان ممدوح حسن، الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني و الدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية و التربوية، عمان، الأردن، 2020، ص 21

2- شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 01، 2020، ص 753.

[3] - أمينة عبيشات، الجرائم الإلكترونية بين المواثيق الدولية والتشريعات الوطنية، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت، المجلد 06، العدد 01، 2021، ص 253.

- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.[1]

كما شملت الإتفاقية على العديد من الجرائم السيبرانية منها:

الولوج غير القانوني، الإعتراض غير القانوني، الإعتداء على سلامة البيانات، الإعتداء على سلامة النظام، إساءة إستخدام أجهزة الحاسب الآلي أو معداتة، الغش الإلكتروني، التزوير الإلكتروني، الجرائم المتصلة بالمواد الإباحية للطفولة، الجرائم المتصلة بالإعتداءات الواقعة على الملكية الفكرية وحقوق المؤلف، الشروع أو الإشتراك.[2]

4- الإتفاقية الأوروبية لحماية الأطفال من الإستغلال و الإعتداء الجنسي:

تم إبرامها في 25 أكتوبر 2007 و التي دخلت حيز النفاذ في جويلية 2010، حيث إشتملت الإتفاقية على مجموعة من التدابير الوقائية المتعلقة أساسا بنشر الوعي بحماية الأطفال من الإستغلال والإعتداء الجنسي، إذ تهدف هذه الإتفاقية إلى منع ومكافحة الإستغلال والإعتداء الجنسيين على الأطفال، وحماية حقوق الأطفال ضحايا الإستغلال و الإعتداء الجنسيين، وكذا تعزيز التعاون الوطني والدولي لمناهضة الإستغلال الجنسي الممارس على الأطفال.

كما ألزمت إتفاقية حماية الأطفال من الإستغلال والإعتداء الجنسي الدول الأطراف بإتخاذ التدابير التشريعية الوقائية اللازمة، وغيرها من التدابير الأخرى، التي تتيح ضمان التعليم المبكر للأطفال، لاسيما خلال المرحلة الابتدائية والثانوية، وتوعيتهم بمخاطر الاستغلال والاعتداء الجنسي خاصة في البيئة الرقمية.[3]

5- إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية:

صدر عن جامعة الدول العربية قانونا إسترشاديا لمكافحة جرائم تقنية الفضاء السيبراني، حيث سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال إستخدام الفضاء السيبراني بالتوقيع على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010/12/21 لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسالمة مجتمعاتها[4].

وتحتوي إتفاقية مكافحة جرائم تقنية المعلومات على 43 مادة حيث تهدف هذه الإتفاقية في الفصل الأول إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطاء هذه الجرائم، حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها و أفرادها، ونجد في الفصل الثاني

---

[1] - أمينة عبيشات، المرجع السابق، ص 254.

[2] - خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في جرائم المعلوماتية - دراسة مقارنة، مكتبة القانون والاقتصاد للنشر والتوزيع، الطبعة الأولى، 2014، ص 33.

[3] - نادية ليتيم، حقوق الطفل بالإتحاد الأوروبي دراسة تحليلية في آليات الحماية القانونية والإستراتيجية، مجلة الحقوق والعلوم الإنسانية، جامعة الشهيد زيان عاشور الجلفة، المجلد 14، العدد 03، 2021، ص 575.

[4] - سليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، جامعة عمار ثليجي الأغواط، المجلد 05، العدد 02، 2022، ص 81.

تفصيلا للأفعال التي تعد مجرمة، أما الفصل الثالث منها فقد تم العرض من خلاله إلى نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع نصت على التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية[1].

كما دعا المجلس الدول العربية المصدقة على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس بإتخاذه من إجراءات لمواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الجرائم الإلكترونية لمنع المجرمين من استخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال الجرائم السيبرانية.

كما دعا المجلس، الدول العربية إلى التعاون لمنع الإرهابيين من إستغلال تكنولوجيا المعلومات والإتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر إستخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود[2].

6- إتفاقية الإتحاد الإفريقي حول الأمن السيبراني و حماية البيانات ذات الطابع الشخصي:

تشكل إتفاقية مالابو نص قانوني إستراتيجي في مجال مكافحة الجرائم السيبرانية في إفريقيا، إذ تعالج مسألة الأمن السيبراني بتوسع، بحيث تضمنت مكافحة الجريمة السيبرانية وحماية البيانات الشخصية والإشراف على المعاملات الإلكترونية وهي تهدف على غرار الإتفاقيات ذات الصلة الى:

- تعزيز وموائمة التشريعات الحالية للدول الأعضاء والمجموعات الإقتصادية الإقليمية في مجال تكنولوجيا المعلومات والإتصالات مع احترام الحريات الأساسية وحقوق الإنسان والشعوب.
- إنشاء وثيقة معيارية مناسبة تتوافق مع البيئة القانونية والثقافية والإقتصادية والإجتماعية الإفريقية.
- التأكيد على حماية البيانات الشخصية والخصوصية.
- تعزيز إستخدام تكنولوجيا المعلومات والإتصالات وزيادة التدفق وإنقاص أسعار الإنترنت
- العمل على تعهد كل دولة طرف بإعتماد تدابير تشريعية و أو تنظيمية لتحديد القطاعات التي تعتبر حساسة لأمنها القومي ورفاهية إقتصادها.
- العمل على تنظيم الإعتراف القانوني بالمعاملات التجارية والعقد والإمضاء الإكترونيين وإيجاد قواعد قانونية تحمي المستهلكين وحقوق الملكية الفكرية والبيانات الشخصية وأنظمة المعلومات.[3]

---

[1] - رانا مصباح عبد المحسن عبد الرازق، آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية"، المجلة القانونية، جامعة القاهرة، المجلد 15، العدد 05، 2023، ص 1390.

[2] - سليمان قطاف، عبد الحليم بوقرين، المرجع السابق، ص 81.

[3] - مريم لوكال، قراءة في إتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية و الإقتصادية، المركز الجامعي سي الحواس بريكة، المجلد 04، العدد 03، 2021، ص 661.

المطلب الثاني:

آليات التعاون الشرطي

تعد الجرائم السيبرانية إحدى أهم صور الجرائم ذات البعد الدولي العابر للحدود، حيث لم تعد تلك الحدود تشكل حاجزاً أمام مرتكبيها، كما أن نشاط هؤلاء الجناة لم يعد قاصرا على إقليم معين بل إمتد إلى أكثر من إقليم، وقد أضحى هناك ضرورة ملحة ومبررات قوية للتعاون أمني دولي لمكافحة الجرائم السيبرانية، بإعتبار أن المجرم السيبراني أصبح مجرما دوليا.

الفرع الأول/ آليات التعاون الشرطي الدولية:

في إطار مواجهة الجرائم السيبرانية و لتعزيز الثقة في البنية التحتية الرقمية تم الإعتماد على آليات التعاون الشرطي الدولية و التي تلعب دورا هاما في مكافحة المخاطر السيبرانية، و تتمثل هذه الآليات في:

1- المنظمة الدولية للشرطة الجنائية (الإنتربول) في مكافحة الجرائم السيبرانية:

أنشأت المنظمة الدولية للشرطة الجنائية (الإنتربول) خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع إستراتيجيات لمواجهة هذا النوع من الجرائم، وذلك من خلال:

- إنشاء مركز إتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة 07 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف.
- إستخدام وسائل حديثة في عملية المكافحة، كإستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج Excalibur للتحليل والمقارنة الأوتوماتيكية لتلك الصور.
- تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيه.[1]

وهكذا يتولى الإنتربول إقامة العلاقات بين الدول والمنظمة، وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بالجرائم المتشعبة في عدة دول، كتلك المتعلقة بالجرائم المعلوماتية.

وبهذا فإن شرطة الإنتربول تعد منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود الوطنية للدول، بما فيها الجرائم السيبرانية، وذلك ما أكدته نتائج الدورة رقم (77) للجمعية العامة لمنظمة الإنتربول، حيث دعا الأمين العام للإنتربول السيد "بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صوره بما فيه الإرهاب

[1] - عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية، جامعة الأزهر، مصر، المجلد 16، العدد 01، 2014، ص 197-198.

السيبراني، وقد نجحت المنظمة الدولية للشرطة الجنائية "الإنتربول" خلال الأعوام الأخيرة في جعلها من أكثر المنضمات الدولية التي يخشاها المجرمون.[1]

2- شرطة الويب الدولية

أنشأت هذه المنظمة الأمنية في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة.

ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم، ونظرا لاتساع نشاط هذه المنظمة وما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خال شبكة الإنترنت على مستوى العالم، و ألا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى.[2]

الفرع الثاني/ آليات التعاون الشرطي الإقليمية:

سعيا لمكافحة الجرائم السيبرانية وإنطلاقا من عائق الحدود الوطنية للدول وسيادتها الإقليمية و نطاق إختصاصها، تم إنشاء أجهزة أمنية ذو طابع إقليمي تتمثل في:

1- آلية الإتحاد الأوروبي للتعاون الشرطي (الأوربول) في مكافحة الجرائم السيبرانية:

مركز الشرطة الأوروبية " الأوروبول " هو أحد الأجهزة الأمنية الأوروبية و الذي يتخد من مدينة لاهاي الهولندية مقر له، و هو مكلف بمكافحة مختلف الإجرام عن طريق:

- معالجة البيانات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوروبي.
- دعم و تشجيع سلطات التحقيق، و ذلك بتكميل وسائلهم و تحديثها من أجل مكافحة جميع أنواع الإجرام المنظم الدولي الخطير.
- تسهيل تبادل المعلومات عن طريق تزويد المحقيقين بتحاليل عملية و إستراتيجية، بالإضافة إلى دعمهم بالخبرات و المساعدات التقنية. [3]

وفي إطار مكافحة الجرائم السيبرانية تم إنشاء **المركز الأوروبي للجرائم الإلكترونية EC3** في عام 2013 من قبل الأوروبول و ذلك لتعزيز تطبيق القانون على الجرائم الإلكترونية في الإتحاد الأوروبي، و بالتالي المساعدة في حماية المواطنين الاوروبيين و الشركات و الحكومات من الجرائم السيبرانية، إذ تقدم مساهمة

[1] - عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 199.
[2] - الطاهر ياكر، مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد 04، العدد 04، 2022، ص 17.
[3] - هشام بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز العربي للدراسات المستقبلية و الإستراتيجية، مصر، 2012. ص 23.

كبيرة في مكافحة الجرائم الإلكترونية بمختلف أشكالها كما يمتد الدعم المقدم أيضا إلى معالجة الإجرام على شبكة الويب المظلمة و المنصات البديلة.

كما أنشأ الأوروبول مع المفوضية الأوروبية و الدول الأعضاء في الإتحاد الأوروبي في عام 2010 **فرقة العمل المعنية بالجرائم الإلكترونية التابعة للإتحاد الأوروبي (EUCTF)**، وهي شبكة قائمة على الثقة يتمثل دورها في تحديد التحديات والإجراءات الرئيسية ومناقشتها وترتيبها حسب الأولوية في مكافحة الجريمة السيبرانية.[1]

2- آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) في مكافحة الجرائم السيبرانية:

آلية الإتحاد الإفريقي للتعاون الشرطي أو ما تعرف إختصارا بـ: "الأفريبول" هي هيئة تقنية لدى الإتحاد الإفريقي ، تهدف إلى إعتماد رؤية شاملة تسمح بتحسين فعالية و نجاعة مصالح الشرطة الإفريقية ، وتتمثل مهمتها في دعم التعاون الشرطي بين الدول الإفريقية من خلال تبادل المعلومات وتعزيز التنسيق فيما بينها ، ولم يتطرق النظام الأساسي " للأفريبول" إلى تعريف هذه الآلية و إكتفى بتسميتها من خلال المادة الأولى بالنص على أن " الأفريبول": (آلية الإتحاد الإفريقي للتعاون الشرطي)، وتتخذ هذه الآلية الجزائر العاصمة مقرا لها ومكانا لعقد دوراتها ، غير أنه يمكن عقد دوراتها في دول أخرى بناءا على طلب إستضافة يقدم من طرف الدولة المعنية [2].

وفي مجال الأمن السيبراني و مكافحة الجرائم الإلكترونية فقد تم إبرام إتفاقية بين الدول الأعضاء في الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، وقد تم من خلال هذه الإتفاقية تحديد التوجهات العامة و الإستراتيجية لمكافحة الجريمة الإلكترونية في إفريقيا.[3]

و في الدورة العاشرة لمنتدى الأمن بإفريقيا التي اختتمت أشغالها في 9 فبراير 2019 بمراكش المغربية و الذي دعى إلى جملة من التوصيات منها إحداث **مرصد إفريقي للأمن الإلكتروني** تكمن مهمته في التنسيق بين الدول الأعضاء في الإتحاد الإفريقي في التصدي للجريمة الإلكترونية وتبادل المعلومات، بالإضافة إلى معالجة الثغرات التي تحول دون ذلك من خلال توحيد التشريعات والسياسات العمومية من أجل أمن إلكتروني إفريقي.[4]

---

[1] - المركز الأوروبي للجرائم الإلكترونية EC3 (التحديث بتاريخ 01 مارس 2022) ، تم الإطلاع عليه بتاريخ :2023/04/17 ، رابط الموقع: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[2] - عزيز لزعر، رشيد زياني، آلية الاتحاد الإفريقي للتعاون الشرطي (الأفريبول) و دورها في مكافحة الجريمة الإلكترونية، مجلة متون، المجلد 14، العدد 03، 2021، ص 254.

[3] - المرجع نفسه، ص 256.

[4] - نفس المرجع، ص 257.

المبحث الثاني:

آليات مكافحة الجرائم السيبرانية على الصعيد الوطني

أضحت الجرائم السيبرانية أحد أهم الهواجس التي تؤثر سلبا على الأفراد في حياتهم الشخصية وحرمة خصوصياتهم من جهة، و الدول و الحكومات في سيادتها و إستقرار شعوبها و أمنها القومي من جهة أخرى، الأمر الذي دفع بالجزائر إلى سن حزمة من التشريعات والآليات القانونية و كذا إستحداث مجموعة من الآليات المؤسساتية للتصدي لهذه لجريمة بمختلف أشكالها.

المطلب الأول:

الآليات التشريعية

لقد حاولت الجزائر كغيرها من الدول سن قوانين خاصة سعيا منها لتجسيد وعيها بأهمية حماية الفضاء الإلكتروني و تعزيز الأمن السيبراني وذلك من خلال مجموعة من القوانين في كل مرة تعدلها أو تلغيها وتضع محلها ما هو أنسب للظروف المعاشة و لتساير التطورات الحاصلة في مجتمعنا وسنتطرف في هذا المطلب إلى أهم النصوص التشريعية و التي لها علاقة مباشر أو غير مباشرة بمكافحة الجرائم السيبرانية.

الفرع الأول/مكافحة الجرائم السيبرانية في إطار القواعد العامة:

أقر المشرع الجزائري مجموعة من التشريعات المرنة التي تساير التطورات المستمرة للجرائم السيبرانية والتي تتمثل في:

01-حماية الحقوق والحريات الفردية من خلال الدستور الجزائري:

من حيث المبدأ الحماية القانونية للحقوق المرتبطة بالحياة الخاصة أو بالخصوصية وكذا الحريات الفردية، يعتبر مبدأ دستوري أقرته معظم الدساتير و التشريعات العالمية، حيث كرس الدستور الجزائري حماية حق الإنسان في حياته وحريته الخاصة من خلال النص على ذلك في الفصل الأول على الحقوق الأساسية والحريات العامة ضمن الباب الثاني المعنون بـ: الحقوق الأساسية والحريات العامة و الواجبات[1]، حيث جاء في نص المادة 35 في فقرتها الأولى ما يلي : "تضمن الدولة الحقوق الأساسية والحريات"، و كذلك من خلال نص المادة 39 منه:" تضمن الدولة عدم انتهاك حرمة الإنسان. يحظر أي عنف بدني أو معنوي، أو أي مساس بالكرامة..." [2]

[1] - زناتي محمد السعيد، جواج يمينة، أثر الجرائم السيبرانية عمى الحريات الفردية (الجزائر نموذجا)، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية أدرار، المجلد 06، العدد 01، 2022، ص 52

[2] - دستور الجزائر لسنة 2020، المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية العدد 82 الصادرة بتاريخ 30 ديسمبر 2020.

كما نص المشرع الجزائري في المادة 47 منه:"لكل شخص الحق في حماية حياته الخاصة وشرفه لكل شخص الحق في سر مراسلاته وإتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الاشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق.."[1]، وعموما نصوص مواد الدستور الجزائري ثرية بحماية الحقوق والحريات الفردية وحرمة الحياة الخاصة.[2]

02-مكافحة الإجرام السيبراني بموجب تعديل قانون العقوبات:

حاول المشرع الجزائري أن يتماشى مع ما هو معمول به في مجال محاربة الإجرام السيبراني بإستحداث نصوص تجرم وتقمع الإعتداءات الواردة على حرية الحياة الفردية عن طريق وسائل وآليات إلكترونية و معلوماتية، بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات، خاصة بسبب التزايد اللامتناهي للاعتداءات على الأنظمة المعلوماتية بتطور آليات الإتصال وظهور مواقع الإلكترونية والإنترنت.[3]

وتضمن القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات قسم عنوانه" المساس بأنظمة المعالجة الآلية للمعطيات ". حيث نصت المادة 394 مكرر منه على ما يلي:" يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عف الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة" تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج.[4]

ذلك مهما كانت قاعدة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الإعتداءات تلك التي تمس ببعض صور الحياة الخاصة.

ونصت المادة 394 مكرر 2 على أنه:" يعاقب... كل من يقوم عمدا وعن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسمة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم،

2-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم "

و تضيف المادة 394 مكرر6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس و الغرامة و بالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية:" يحكم بمصادرة الأجهزة و البرامج و الوسائل

[1] - دستور الجزائر لسنة 2020، المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية العدد 82 الصادرة بتاريخ 30 ديسمبر 2020.
[2] - زناتي محمد السعيد، جواج يمينة، المرجع السابق، ص 52 – 53.
[3] - المرجع نفسه، ص 53.
[4] - قانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66 – 156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 الصادر بتاريخ 10 نوفمبر 2004

المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها. "[1]

و في سنة 2006 قام المشرع بإدخال تعديلات جديدة قانون العقوبات المعدل بالقانون رقم 06-23 مست القسم السابع مكرر منه حيث تم تشديد العقوبة على كل الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها، و يعود ذلك بالتأكيد إلى إقرار المشرع بأن الظاهرة جديدة ومستحدثة متميزة عن الجرائم التقليدية من حيث محلها وأشخاص مرتكبيها، و سعيا منه في ضمان المكافحة لم يميز بين نوعية المعلومات التي تطالها الحماية سواء كانت مادية أو اقتصادية أو مسائل أمنية غرضها في ذلك هو حتما تحقيق الردع العام على اثر التزايد الخطير لنسب الجرائم المرتكبة و تنوعها و خطورتها على الأفراد من جهة وعلى الاقتصاد الوطني من جهة أخرى.[2]

كما قام المشرع الجزائري في سنة 2014 بتعديل قانون العقوبات من خلال القانون رقم 14-01 مؤرخ في 4 فبراير سنة 2014، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، و ذلك بإضافة المادة 333 مكرر 1 من القسم الثاني (في ترك الأطفال والعاجزين وتعريضهم للخطر وبيع الأطفال) من الفصل الثاني (الجنايات والجنح ضد الأسرة والآداب العامة) من الباب الثاني (الجنايات والجنح ضد الأفراد) من الكتاب الثالث (الجنايات والجنح وعقوباتها).[3]

حيث جرمت المادة 333 مكرر 1 ق ع، تصوير قاصر لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر.[4]

أما التعديل الذي أقره القانون رقم 16-02 المؤرخ في19 يونيو 2016 المعدل لقانون العقوبات قد أضاف المادة 87 مكرر11 التي تعاقب كل جزائري أو أجنبي يرتكب أفعالاً إرهابية، أو يدبرها أو يعد لها أو يشارك فيها أو يدرب عليها أو يتلقى تدريبا عليها، ...يستخدم تكنولوجيات الإعلام والإتصال لإرتكاب الأفعال المذكورة في هذه المادة.[5]

[1] - - زناتي محمد السعيد، جواج يمينة، المرجع السابق، ص 54

[2] - سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، المجلد ب، العدد 52، 2019، ص 49

[3] - قانون رقم 14-01 المؤرخ في 04 فيفري 2014، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 07 الصادر بتاريخ 16 فيفري 2014.

[4] - وردة شرف الدين، سامية بلجراف، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، جامعة يحي فارس المدية، المجلد 01، العدد 03، 2017، ص 37.

[5] - قانون رقم 16-02 المؤرخ في 19 جوان 2016، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 37 الصادر بتاريخ 22 جوان 2016.

وأضاف التعديل المذكور المادة87 مكرر12 التي تنص على أن القانون يعاقب كل من يستخدم تكنولوجيات الإعلام والاتصال من أجل دعم تلك الأعمال أو تنظيمها أو نشر أفكارها بطريقة مباشرة أو غير مباشرة، أو تجنيد الأشخاص لصالح جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها الإرهاب. وبالتالي يتبين أن الأسلحة الإلكترونية المستعملة في الجريمة السيبرانية صارت بديلا عن التهديدات التقليدية لأنه لا يحتاج إلى حدود جغرافية، ولا توجد وسائل مراقبة لتحديد هويته في الشبكة العنكبوتية على غرار الحروب التقليدية.[1]

03-مكافحة الإجرام السيبراني بموجب تعديل قانون الإجراءات الجزائية:

وسعت المادة 16 من قانون الإجراءات الجزائية الإختصاص المحلي لضباط الشرطة القضائية فيما يتعلق بالبحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وذلك بتمديد الإختصاص إلى كامل الإقليم الوطني، كما جاءت المادة 37 من قانون الإجراءات الجزائية و المادة 40 منه لتمكن كل من وكيل الجمهورية وقاضي التحقيق على تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

حيث قام المشرع الجزائري بموجب القانون رقم 04-14 المتضمن تعديل قانون الإجراءات الجزائية بإنشاء المحاكم ذات الإختصاص المحلي الموسع أو ما يعرف بالأقطاب الجزائية المتخصصة[3]، بحيث تم تمديد الإختصاص لبعض المحاكم المذكورة على سبيل الحصر للنظر في بعض الجرائم المحددة و منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[4]

كما تم إستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و ذلك بموجب الأمر رقم 21-11 المتمم للأمر رقم 66-155 المتضمن لقانون الإجراءات الجزائية و الذي يتممه بباب سادس عنوانه " القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" و الذي يتضمن المواد 211 مكرر 22 و211 مكرر23 و211 مكرر 24 و211 مكرر 25 و211 مكرر 26 و211 مكرر 27 و211 مكرر 28 و211 مكرر29 .حيث يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني وهذا طبقا للمادة 211 مكرر23.[5]

---

[1] - جيلالي دلالي، يعقوب بلبشير، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، مجلة كلية القانون الكويتية العالمية، المجلد 10، العدد 01، 2021، ص 557

[2] - فاروق خلف، المرجع السابق، ص 17.

[3] - قانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 71 الصادر 10 نوفمبر 2004.

[4] - بوعزة نضيرة، المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث و الدراسات، المركز الجامعي عبد الحفيظ بوصوف ميلة، المجلد 07، العدد 01، 2021، ص 184.

[5] - أمر رقم 21-11 المؤرخ في 25 أوت 2021، المتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 65 الصادرة بتاريخ 26 أوت 2021.

الفرع الثاني/ مكافحة الجرائم السيبرانية في إطار القوانين الخاص:

لقد أقر المشرع الجزائري صكوكا قانونية في مكافحة الجرائم السيبرانية متمثلة أساسا في:

01-الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة:

نص المشرع الجزائري في الأمر رقم 03-05 على مجموعة من المصنفات الأدبية و الفنية تاركا المجال لظهور مصنفات جديدة قد تبرزها التكنولوجيا مستقبلا، و نص على نوعين من المصنفات الرقمية هما: برامج الحاسوب في المادة 04 منه و قواعد البيانات في المادة 05.[1]

و يعرف المصنف الرقمي بأنه:" كل عمل إبداعي ينتمي إلى بيئة تكنولوجيا المعلومات، أو ما يصطلح على تسميتها بالبيئة الرقمية"[2]

حيث أقر المشرع الجزائري في الأمر 03-05 حماية قانونية على المصنفات الرقمية سواء برامج الحاسوب أو قواعد البيانات، و ذلك بتوفر شرطي الابتكار و التعبير عنه، و قد جرم تقليد المصنفات الرقمية و تداول النسخ المقلدة، فسلط على مرتكبيها عقوبات جزائية و أخرى مدنية تهدف لتعويض المتضرر عن المساس بحقوقه المعنوية و المالية، كما أمكن للمؤلف و ذلك قبل الفصل في أي دعوى طلب إجراءات تحفظية لدفع أي اعتداء محتمل الوقوع على مصنفه الرقمي.[3]

و عليه فإن حماية مواقع الإنترنت في الفضاء السيبراني التي تستغل مصنفا أدبيا أو فنيا بموجب قانون حق المؤلف و الحقوق المجاورة ينتج عنه حماية الحق الأدبي و المالي للموقع المسجل كمصنف، و حماية قانونية لأي حق آخر يتم الإعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الإسم و الصورة و المعلومات الخاصة... و في كل الأحوال لا يمكن الفصل بين حماية المصنف المستغل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف و الحقوق المجاورة في الوقت نفسه، لأن حماية الموقع تؤدي بالضرورة إلى عدم الإعتداء على محتوياته بما في ذلك المصنف وغيره من الحقوق و الحريات الفردية التابعة له.[4]

02-مكافحة الإجرام السيبراني بموجب قانون 08-01 الخاص بالتأمينات الإجتماعية:

جاء القانون رقم 08-01 المؤرخ في 23 يناير 2008 والمتعلق بالتأمينات الإجتماعية المتمم لأحكام القانون 83-11 المؤرخ في 02 يوليو 1983 بباب خامس مكرر عنوانه "أحكام جزائية" يتضمن المواد:

---

[1] - الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى سنة 1424 الموافق 19 يوليو عام 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية العدد 44 الصادر بتاريخ 23 يوليو 2003.

[2] - عيساني طـــه، عبد الله فوزية، المصنفات الرقمية المشمولة بالحماية بموجب قوانين الملكية الفكرية في الاتفاقيات الدولية والقانون الجزائري، دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، المجلد 13، العدد 10، 2021، ص 134.

[3] - صفرة بشيرة، حماية المصنفات الرقمية في التشريع الجزائري، مجلة الحقوق و العلوم الإنسانية، جامعة الجلفة، المجلد 01، العدد 29، 2016، ص 280.

[4] - زناتي محمد السعيد، جواج يمينة، المرجع السابق، ص 56.

93 مكرر2، 93 مكرر 3، 93 مكرر4، 93 مكرر 5، 93 مكرر 6، و تتمثل الجرائم المعلوماتية التي ترتكب على البطاقة الإلكترونية للمؤمن له إجتماعيا فيما يلي:[1]

- تسليم أو إستلام بهدف الإستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة المادة 93 مكرر 2.[2]
- القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة المادة 93 مكرر 1/3.
- الإعداد أو التعديل أو النسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو بإستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة.[3]

03-مكافحة الإجرام السيبراني بموجب القانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

تواكبا مع التطورات التي عرفتها الجزائر في مجال تطور التقنية والتكنولوجيا، ولأنها في الغالب أصبحت محلا للجريمة باشر المشرع الجزائري إجراءات جديدة للمواجهة تضمنت إصدار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، و هو القانون المنظم للفضاء الإلكتروني بصفة عامة ومكافحة المجال الإجرامي المتصل به من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة.

يتكون القانون من ست فصول تتضمن تعريفا للجريمة المعلوماتية والتي لم تختلف كثيرا عما ورد في قانون العقوبات، أيضا بعض الأحكام المتعلقة بمراقبة الاتصالات الإلكترونية وأيضا القواعد الإجرائية لتفتيش المنظومات المعلوماتية، إضافة إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.[4]

ولعل أهم ما يثيره هذا القانون بالرغم من أنه جاء لتكملة سلسلة الترسانة القانونية لمواجهة الإشكالات القانونية التي ترتبط بتنوع الجريمة الإلكترونية وتطورها المستمر، بالرغم من ذلك يبقى الفصل الثاني من هذا القانون بقلق الحقوقيين بدعوى أن هذا القانون يجيز مراقبة الاتصالات الفردية من دون علم الأفراد ومن دون

[1] - قانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11 المؤرخ في 02 يوليو 1983 المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية عدد 04 الصادرة بتاريخ 27 يناير 2008.

[2] - سليمان قطاف، عبد الحليم بوقرين، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المركز الجامعي بآفلو، المجلد 06، العدد 01، 2022، ص 350.

[3] - المرجع نفسه، نفس الصفحة.

4 - سعيدة بوزنون، المرجع السابق، ص 50.

إرتكاب أي نوع من الإجرام المادي أو المعنوي و هو ما يشكل خرقا للحق في الخصوصية و إنتهاكا لحقوق الإنسان وقرينة البراءة المكفولة دستوريا.

إن الظاهر من النص يوحي بأن القانون يتضمن انتهاكا صارخ للحق في الخصوصية، ولكن الواضح أن هناك ما يبرره في الغالب و هو مضمون المادة 4 من القانون 09-04 التي نصت على أربع حالات يجوز فيها فقط اللجوء إلى إجراء وذلك بالنظر إلى خطورة التهديدات المحتملة و لأهمية المصلحة المحمية منها:

- جرائم الإرهاب و التخريب وجرائم ضد أمن الدولة.
- توفير معلومات عن إحتمال وقوع إعتداء على منظومة معلوماتية تهدد مؤسسات الدولة أو الدفاع الوطني.
- ضرورات التحقيق والمعلومات القضائية.
- تنفيذ طلبات المساعدات القضائية بين الدول.[1]

04-مكافحة الإجرام السيبراني بموجب القانون رقم 15 – 04 الذي يحدد القواعد العامة المتعمقة بالتوقيع والتصديق الإلكترونيين:

أنشأ في هذا المجال ما يسمى بمزود خدمة للمصادقة الإلكترونية، والذي يفي بعدد من الالتزامات القانونية لخلق بيئة إلكترونية آمنة للمعاملات عبر الإنترنت. ولحماية المستهلك الإلكتروني من مخاطر السلع والخدمات التي يحصل عليها، و منعه من الوقوع ضحية للعقود الإلكترونية.[2]

حيث يساهم القانون 15-04 الخاص بالتوقيع والتصديق الإلكترونيين في حماية الوثيقة الإلكترونية، من خلال إعطاء صفة الرسمية للوثيقة الإلكترونية واستعمالها في النشاط الإداري داخل المؤسسات والإدارات العمومية و الخاصة، إضافة إلى تعيين سلطات التوقيع الإلكتروني وتحديد مهامها وآلية حماية الوثيقة الإلكترونية من خلال التوقيع والتصديق الإلكترونيين.[3]

05-مكافحة الإجرام السيبراني بموجب القانون رقم 15-12 المتعلق بحماية الطفل:

نص المشرع الجزائري على قانون حماية الطفل رقم 15-12 والذي يحمل في طياته قواعد قانونية إجرائية وعقابية وذلك لحماية الطفل من مختلف المخاطر التي تحيط به، حيث نص في المادة 02 منه:".... الطفل في خطر": الطفل الذي تكون صحته أو أخلاقه أو تربيته أو أمنه في خطر أو عرضة له، أو تكون ظروفه المعيشية أو سلوكه من شأنهما أن يعرضاه للخطر المحتمل أو المضر بمستقبله، أو يكون في بيئة تعرض سلامته البدنية أو النفسية أو التربوية للخطر.[4]

---

[1] - سعيدة بوزنون، المرجع السابق، ص 50

[2] - سليمان قطاف، عبد الحليم بوقرين، المرجع السابق، ص 351.

[3] - كحيلة سارة، أمن وحامية الوثائق الإلكترونية من خلال المعايير الدولية والنصوص التشريعية، Aleph. Langues, Medias et sociétés ، جامعة الجزائر 2، المجلد 08، العدد 03، 2021، ص 515.

[4]- قانون رقم 15-12 مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015، يتعلق بحماية الطفل، الجريدة الرسمية الجزائرية عدد 39 الصادر بتاريخ 19 يوليو 2015.

كما أدرج نفس القانون في المادة 02 حماية الطفل من الإستغلال الجنسي بمختلف أشكاله، وذلك من خلال إستغلاله لاسيما في المواد الإباحية وفي البغاء وإشراكه في عروض جنسية و إعتبارها من حالات تعريض الطفل للخطر.[1]

كما تطرقت المادة 141 على عقوبة إستغلال الطفل عبر وسائل الإتصال في مسائل منافية للآداب العامة والنظام العام حيث تنص المادة 141: دون الاخلال بالعقوبات الأشد، يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 150.000 دج إلى 300.000 دج، كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب العامة والنظام العام.

06-مكافحة الإجرام السيبراني بموجب القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكتروني:

حيث إستحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الإفتراضي منها، إستحداث سلطة ضبط من بين مهامها السهر على إحترام متعاملي البريد والإتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والإتصالات الإلكترونية والأمن السيبراني و ذلك طبق للمادة 13 من القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية.[2]

كما جرم إنتهاك سرية المراسلات المرسلة عن طريق البريد أو الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو إستعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في إرتكاب هذه الجريمة.[3]

07-مكافحة الإجرام السيبراني بموجب القانون 18 – 05 المتعلق بالتجارة الإلكترونية:

نص المشرع الجزائري في المادة 03 من قانون 18-05 على ما يلي: "تمارس التجارة الإلكترونية في إطار التشريع والتنظيم المعمول بهما.

غير أنه، تمنع كل معاملة عن طريق الإتصالات الإلكترونية تتعلق بما يأتي: .....

- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية،
- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به، ....."[4]

[1] -حليمة بن دريس، حماية الأطفال ضحايا الجرائم الإلكترونية، مجلة المفكر للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، العدد 06، 2019، ص 235.

[2] - قانون رقم 18-04 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية عدد 27، الصادرة بتاريخ 13 ماي 2018.

[3] - رضا مهدي، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المركز الجامعي المقاوم الشيخ آمود بن مختار إليزي، المجلد 06، العدد 02، 2021، ص 121.

[4] - قانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد 28، الصادرة بتاريخ 16 ماي 2018.

كما تنص المادة 05 منه:" تمنع كل معاملة عن طريق الإتصـالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به، وكذا كل المنتجات و/أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي"[1].

كما أقر المشرع الجزائري في هذا الباب إلى ضرورة الرقابة لزرع الثقة لدى المتعاملين عبر الانترنيت في مجال التبادل التجاري الالكتروني حيث أكد أن كل أعمال المورد الإلكتروني تخضع إلى رقابة ضباط وأعوان الشرطة وكذا رقابة الأعوان المنتمون للأسلاك الخاصة بالرقابة التابعون للإدارات المكلفة بالتجارة، وتبعا لطبيعة الجرائم يتم التخطيط لغرامات تتراوح بين 50 ألف دينار و 2 مليون دينار، دون الإخلال بتطبيق كامل أكثر صرامة في حالة بيع سلع وخدمات ممنوعة من التسويق حيث يعاقب بغرامة مالية من 200 ألف دينار إلى مليون دينار مع الشطب من السجل التجاري وإغلاق الموقع نهائيا ، أما الأشخاص الطبيعيون أو المعنويين الذين يزاولون نشاط تجاري عبر الانترنيت دون سجل إلكتروني يتم تعليق موقعهم إلى غاية تسوية وضعيتهم، كما يضاعف مبلغ الغرامة في حال تكرار نفس الجريمة خلال مدة ال تتجاوز 12 شهرا من تاريخ العقوبة السابقة.[2]

08-مكافحة الإجرام السيبراني بموجب القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

أصدر المشرع الجزائري القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من أجل سد الفراغ التشريعي ولضمان الحماية القانونية للحياة الشخصية للأفراد ومنها المعطيات ذات الطابع الشخصي، وليتصدى لآثار التقدم السريع لتكنولوجيا الإعلام و الإتصال، إذ يهدف القانون 18-07 المؤرخ في 2018/06/10 إلى تحديد قواعد حماية الأشخاص الطبيعيين ذات الطابع الشخصي من أي انتهاكات مهما كان مصدرها أو شكلها في إطار احترام الكرامة الانسانية والحياة الخاصة والحريات العامة، وألا تمس حقوق الأشخاص وشرفهم و سمعتهم ، وهذا تماشيا مع مبادئ الدستور الذي يكرس مبدأ احترام القانون، ويشدد على أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني الذي يمكنه التراجع عن موافقته في أي وقت. وذلك من خلال تعريف المعطيات الشخصية وحقوق الشخص المعني، وكذا التطرق إلى الحماية الإدارية عن طريق **السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، وكذا النص على الجرائم المتعلقة بمخالفة القواعد الموضوعية والقواعد الإجرائية المنصوص عليها في القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3] .

---

[1] - قانون رقم 18-05، المرجع السابق.

[2] - نجود حمري، نوال حمري، واقع التجارة الالكترونية في الجزائر وفق مقتضيات قانون رقم 18- 05(قانون التجارة الالكترونية) ، مجلة البحوث القانونية والاقتصادية، المركز الجامعي بآفلو، المجلد 04، العدد 01، 2021، ص 19.

[3] - كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية لقانون الأعمال، جامعة محمد بوضياف المسيلة، المجلد 01، العدد 02، 2020، ص 52.

09-مكافحة الإجرام السيبراني بموجب القانون 23 – 04 المتعلق بالوقاية من الإتجار بالبشر ومكافحته:

أقر المشرع الجزائري قانون رقم 23-04 والذي يهدف إلى الوقاية من الإتجار بالبشر ومكافحته، حيث نص في المادة 02 منه على: "يقصد في مفهوم هذا بما يأتي:

1- **الإتجار بالبشر:** تجنيد أو نقل أو تنقيل أو إيواء أو إستقبال شخص أو أكثر بواسطة التهديد بالقوة أو بإستعمالها أو غير ذلك من أشكال الإكراه أو الإختطاف، ..... بقصد الإستغلال.
ويشمل الإستغلال، خصوصا، إستغلال دعارة الغير أو سائر أشكال الإستغلال الجنسي ..... .

4-**الإستغلال الجنسي:** الحصول على مزايا مهما كانت طبيعتها سواء من وضع شخص في تعاطي الدعارة أو أي نوع من الخدمات الجنسية، ولاسيما إستغلاله في مشاهد إباحية من خلال إنتاج وحيازة وتوزيع بأي وسيلة مشاهد أو مواد إباحية....." [1]

وفي إطار إجراءات البحث و التحري للكشف عن جرائم الإتجار بالبشر و معاقبة مرتكبيها يمكن للجهات القضائية أن تأمر مقدمي الخدمات أو أي شخص آخر بتسليمها معلومات أو معطيات ذات صلة تكون مخزنة بإستعمال وسائل تكنولوجيات الإعلام و الإتصال، و ذلك تحت طائلة العقوبات المنصوص عليها في هذا القانون، و هذا ما نستشفه من خلال نص المادة 31 منه.

كما نصت المادة 32 منه على إجراء التسريب الإلكتروني كإجراء خاص للتحري والتحقيق يمكن من خلاله لضابط الشرطة القضائية بموجب إذن قضائي أن يلجأ إلى كل منظومة معلوماتية أو أي نظام اتصال إلكتروني آخر يسمح بمراقبة المشتبه فيهم.

كما أقر نفس القانون في المادة 33 ، لوكيل الجمهورية أو قاضي التحقيق "صلاحية الترخيص للشرطة القضائية بتحديد الموقع الجغرافي للمشتبه فيهم والمتهمين أو وسيلة الجريمة أو أي بضاعة أو أي شيء آخر له صلة بالجريمة من خلال استعمال وسائل تكنولوجيات الإعلام والاتصال عن طريق منظومة المعلوماتية أو بوضع ترتيبات تقنية معدة خصيصا لهذا الغرض.

كما يمكن لضباط الشرطة القضائية المختصة وضع تقنيات للتبليغ عن الجرائم الإتجار بالبشر عبر شبكة الإنترنت، حيث نصت المادة 34 منه: "يمكن ضابط الشرطة القضائية المختص وضعّ آليات تقنية للتبليغ عن جريمة من الجرائم المنصوص عليها في هذا القانون، عبر الشبكة الإلكترونية، ويعلم بذلك فورا وكيل الجمهورية المختص الذي يأمر بالاستمرار في العملية أو بإيقافها". [2]

[1] - قانون رقم 23-04 المؤرخ في 07 ماي 2023، المتعلق بالوقاية من الإتجار بالبشر ومكافحته، الجريدة الرسمية عدد 32، الصادرة بتاريخ 09 ماي 2023.
[2] - المرجع نفسه.

المطلب الثاني:

الآليات المؤسساتية الوطنية

خلقت الجريمة السيبرانية تحديات كبرى أمام الدولة وعلى اعتبار أنها حديثة الظهور فإن هذا يجعلها ذات خصوصية تميزها عن الجرائم التقليدية ما جعل الأنظمة القانونية تصطدم مع حقيقة قصور الجهات الأمنية التقليدية المكلفة بمكافحة الجريمة للتصدي للجريمة السيبرانية وعدم القدرة على تغطية مختلف جوانبها الأمر الذي جعلها تتفشى بصورة كبيرة وسريعة وترتب مع ضرورة العمل على استحداث جهات وأجهزة حديثة تتناسب مهامها والوسائل الموكلة لها مع خصوصية الجريمة السيبرانية وتساعد على التصدي لها وفق ما هو واجب ومأمول.

الفرع الأول/ الجهات المكلفة بمكافحة الجرائم السيبرانية

تتمثل الجهات المكلفة بمكافحة الجرائم السيبرانية في:

01-الديوان الوطني لحقوق المؤلف و الحقوق المجاورة:

أنشئ الديوان الوطني لحقوق المؤلف و الحقوق المجاورة بموجب الأمر 49/73 المؤرخ في 1973/7/29 و أعيدت هيكلته بموجب المرسوم التنفيذي 366/98، ثم بموجب المرسوم 356/05 المؤرخ في 2005/09/21[1]، و هو مؤسسة عمومية ذو طابع صناعي و تجاري، يتمتع بالشخصية المعنوية و الإستقلال المالي، و يعمل تحت وصاية وزارة الثقافة.

وقد خول لهذا الأخير مهمة معاينة أي مساس بحقوق الملكية الفنية و الأدبية لأصحاب المصنفات الرقمية ضحايا القرصنة و التقليد، و تمديد اختصاصه لحد حجز النسخ المقلدة و المزورة ووضعها تحت سلطة الديوان و القيام بإخطار فوري لرئيس الجهة القضائية المختص التي تفصل في خلال 03 أيام في طلب الحجز التحفظي.[2]

02-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

حيث استحدثت هذه الهيئة بموجب القانون 09-04 وبقيت تشكيلتها وتنظيمها و كيفيات سيرها لتحدد عن طريق التنظيم والذي توالت فيه التغييرات ابتداء من المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08 ثم سنة 2019 ليصدر المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020 ،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ليعيد تنظيم الهيئة،

[1] - مرسوم تنفيذي رقم 05-356 المؤرخ في 21 سبتمبر 2005، المتضمن القانون الأساسي للديوان الوطني لحقوق المؤلف و الحقوق المجاورة و تنظيمه و سيره، الجريدة الرسمية الجزائرية عدد 65 الصادر بتاريخ 21 سبتمبر 2005.

[2] - عميش وهيبة، دور الهيئات الوطنية لحماية المصنفات الرقمية في القانون الجزائري، القانونية الدراسات القانونية، المجلد 08، جامعة يحي فارس المدية، العدد 01، 2022، ص 385.

وعرفها بأنها: سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة رئيس الجمهورية، ويحدد مقرها في الجزائر العاصمة، ويمكن نقله الى أي مكان من التراب الوطني بموجب مرسوم رئاسي[1]، و تتكون الهيئة من مجلس توجيه و مديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية و يقدمان عرضا عن نشاطاتهما.[2]

و من مهام الهيئة أن تتصدى لطائفة من الجرائم السيبرانية من خلال تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، و القيام بمساعدة السلطات القضائية و مصالح الشرطة في التحريات التي تجريها بشأنها، و ضمان مراقبة الإتصالات الإلكترونية أيضا قصد الكشف عن طائفة من الإجرام الخطير الذي من شأنه المساس بكيان الدولة و أمنها.

و من المهام الملقاة على عاتق الهيئة أيضا تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل إستعمالها في الإجراءات القضائية، و تعمل في ذات الوقت على تطوير مجال تعاونها مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي في سبيل أداء مهامها مؤهلة بأن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها.[3]

كذلك تقوم الهيئة بالسهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال إختصاصها، كما يقع على كاهل الهيئة المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية مما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة وإقتدار.[4]

03-الهيئة الوطنية لحماية وترقية الطفولة:

تعتبر هذه الهيئة من أهم الجهات المكلفة بحماية الطفل والعمل على مكافحة كل صور الإنتهاكات التي من شأنها المساس بسلامته، وتم استحداثها لهذا الغرض بموجب المادة 11 من القانون 15-12 التي نصت على: "تحدث، لدى الوزير الأول، هيئة وطنية لحماية وترقية الطفولة يرأسها المفوض الوطني لحماية الطفولة، تكلف بالسهر على حماية وترقية حقوق الطفل، تتمتع بالشخصية المعنوية والاستقلال المالي.

تضع الدولة، تحت تصرف الهيئة الوطنية لحماية وترقية الطفولة، كل الوسائل البشرية والمادية اللازمة للقيام بمهامها.

---

[1] - المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 40 الصادرة بتاريخ 18 يوليو 2020.

[2] - رضا مهدي، المرجع السابق، ص 120.

[3] - عائشة شيخي، عياشي بوزيان، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و أشكالها الإقتصادية و آليات مكافحتها، مجلة الدراسات الحقوقية، جامعة الدكتور الطاهر مولاي سعيدة، العدد الرابع، 2015، ص 176.

[4] - المرجع نفسه، ص 177.

تحدد شروط وكيفيات تنظيم الهيئة الوطنية لحماية وترقية الطفولة وسيرها عن طريق التنظيم".[1] وعليه تم إصدار المرسوم التنفيذي رقم 16– 334 المحدد لتشكيلة الهيئة و الأحكام المتعلقة بها:

أ- تشكيلة الهيئة الوطنية لحماية وترقية الطفولة:

طبقا للمرسوم التنفيذي رقم 16– 334 فإن الهيئة تتشكل من مجموعة من الأقسام والمديريات التي توضع تحت رئاسة وإشراف رئيس الهيئة الذي اصطلح عليه بموجب القانون **بالمفوض الوطني لحماية وترقية الطفولة** والذي يتم تعيين وجب مرسوم رئاسي من بين الشخصيات الوطنية ذات الخبرة والكفاءة المعروفة في مجال الإهتمام بالطفولة، وتوضع تحت رآسة المفوض الوطني لحماية وترقية الطفولة مجموعة من الأقسام التي تساعده في القيام بالمهام الموكلة إليه بموجب القانون والمتمثلة في: الأمانة العامة، مديرية حماية حقوق الطفل، مديرية ترقية حقوق الطفل، لجنة التنسيق الدائمة واللجان الموضوعاتية.[2]

ب- إختصـــاصـــات الهيئة الوطنية لحماية وترقية الطفولة:

يدخل دور الهيئة في حماية الطفل من خطر الجرائم السيبرانية ويمكن حصر هذه الإختصاصات فيما يلي:

1-**التخطيط و التنظير**: من بين الإختصاصات الموكلة للهيئة الوطنية لحماية وترقية الطفولة مهمة التخطيط بوضع برامج وطنية و محلية و ترقية حقوق الطفل من خلال التنسيق بين مختلف المتعاملين مع الطفل، حيث أوكلت هذه المهمة بالتحديد للمفوض الوطني لحماية وترقية الطفولة، والذي يتولى مهمة التخطيط و التنظير من خلال متابعة الأعمال المباشرة ميدانيا في مجال حماية الطفل وضمان حقوقه.[3]

2-وضـعية الطفل عبر الإنترنت: من بين أهم اختصاصات الهيئة هو منحها الدور الرئيسي في تكريس حماية حقوق الطفل في العالم الرقمي عن طريق وضع نظام معلوماتي وطني حول وضعية الطفولة والطفل في الجزائر في جميع المجالات وعلى جميع المستويات، مع ضرورة التنسيق مع مختلف الإدارات والهيئات المعنية التي تتولى مهمة تزويد الهيئة بجميع المعلومات التي من شأنها المساهمة في حماية الطفل من صور الإعتداءات والانتهاكات التي تمس بسلامة الجسدية والنفسية.[4]

3-إجراءات التدخل: طبقا للمادة 19 من المرسوم التنفيذي رقم 16-334 فإنه يمكن إدراج مجموعة من الإجراءات التي تدخل في صلاحيات الهيئة لحماية الطفل ومنها:[5]

---

[1] - قانون رقم 15-12 مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015، يتعلق بحماية الطفل، الجريدة الرسمية الجزائرية عدد 39 الصادر بتاريخ 19 يوليو 2015.

[2] - سمية بهلول، الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال و مكافحتها، مجلة العلوم القانونية و الإجتماعية، جامعة زيان عاشور الجلفة، المجلد 06، العدد 04، 2021، ص 308.

[3] - حسينة شرون، فاطمة قفاف، الدور الحمائي للهيئة الوطنية لحماية و ترقية الطفولة، حوليات جامعة الجزائر 1، الجزء الثاني، العدد 32، 2018، ص 547.

[4] - سمية بهلول، المرجع السابق، ص 308-309.

[5] - مرسوم تنفيذي رقم 16-334 المؤرخ في 19 ديسمبر 2016 يحدد شروط و كيفيات تنظيم و سير الهيئة الوطنية لحماية و ترقية الطفولة، الجريدة الرسمية عدد 75 الصادرة بتاريخ 21 ديسمبر 2016.

أ) **الإخطار:** ويتولى المفوض الوطني مسألة الإخطار بأي وسيلة من طرف الطفل أو ممثله الشرعي . أو أي شخص طبيعي أو معنوي، كما يمكن أن يتدخل تلقائيا لمساعدة الأطفال في خطر أو في حالات المساس بمصلحته، حيث تم تزويد الهيئة برقم أخضر مجاني"1111" من شأنه تسهيل عملية الإخطار.[1]

ب) **التحقيق:** إضافة إلى الإخطار ضمن المشرع إجراءات تحقيق مضبوطة للهيئة الوطنية لحماية وترقية الطفولة، تخول من خلالها الهيئة صلاحية التحقيق في التبليغات المتعلقة بإنتهاكات حقوق الطفل عبر مصالح الوسط المفتوح التي يتوجب عليها في هذا الشأن إتخاذ جميع الإجراءات اللازمة لإنقاذ وحماية الطفل من الخطر في حالة ثبوت وجوده.[2]

04-السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

هي سلطة إدارية هي مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي والإداري تنشأ لدى رئيس الجمهورية مقرها بالجزائر العاصمة ، تتكون من 13 عون يعينون بمرسوم رئاسي لعهدة مدتها 05 سنوات قابلة للتجديد ، تضطلع السلطة الوطنية حسب ما حددته المادة 25 من القانون 18 -07[3] بجملة من المهام من بينها السهر على مطابقة ومعالجة المعطيات ذات الطابع الشخصي ، وضمان عدم إنطواء أخطار إستعمال تكنولوجيا الإعلام والإتصال على حقوق الأشخاص والحريات العامة والخاصة، ومنح التراخيص وتقدم الإستشارات للأشخاص والكيانات التي تلجأ الى معالجة المعطيات ذات الطابع الشخصي، والترخيص بنقل المعطيات نحو الخارج في حال كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الاساسية للأشخاص إزاء المعالجة التي تضع لها هذه المعطيات حسب ما نصت عليه المادة 44 ، وتقديم أي إقتراح من شأنه تبسيط وتحسين الإطار التشريعي وتنظيمي لمعالجة المعطيات، وتطوير علاقات التعاون مع السلطات الأجنبية المماثلة و إصدار عقوبات إدارية ، كما تتمتع بالعديد من المهام الأخرى ، كما تعد السلطة الوطنية تقريرا سنويا مفصلا حول جميع نشاطاتها وترفعه إلى رئيس الجمهورية ، كما يلزم رئيس السلطة وأعضائها حسب المادة 26 بالمحافظة على الطابع السري للمعطيات وكل المعلومات التي اطلعوا عليها ولو بعد إنتهاء مهامهم.[4]

---

[1] - حسينة شرون، فاطمة قفاف، المرجع السابق، ص 547

[2] - سمية بهلول، المرجع السابق، ص 309.

[3] - قانون رقم 18-07 المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 الصدرة بتاريخ 10 جوان 2018.

[4] - محمد العيداني، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي علي كافي تندوف، العدد 05، 2018، ص 123.

الفرع الثاني/ الأجهزة الأمنية المتخصصة في مكافحة الجريمة السيبرانية

تتمثل الأجهزة الأمنية المتخصصة في مكافحة الجريمة السيبرانية في:

01- الوحدات التابعة للأمن الوطني:

في سبيل مكافحة الجريمة السيبرانية عملت وزارة الداخلية والجماعات المحلية إلى إنشاء وحدات تابعة لسلك الأمن الوطني والتي تم على مستواها إستحداث:

أ) المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

إستجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.[1]

ب) مصلحة نيابة مديرية الشرطة العلمية والتقنية:

هذه الأخيرة تتكون من المخبر المركزي للشرطة العلمية والذي تم تحديد مقره بالجزائر العاصمة إلى جانب أربع (04) مخابر جهوية مقرها كل من قسنطينة، وهران، بشار و تمنراست و تم على مستوى هذه المخابر إنشاء دائرة علمية ودائرة تقنية مكلفة بمهام التحري والتحقيق وتحليل الأدلة الجنائية المتحصل عليها من ارتكاب الجريمة السيبرانية.

كما تضم المخابر عدة فروع من بينها فرع علم الأدلة الجنائية الحاسوبية والذي يعهد إلى متابعة الجرائم السيبرانية والتحري عنها والعمل على مكافحتها والوقاية منها وذلك عن طريق دراسة وتحليل نوعية خاصة من الأدلة المسماة الأدلة العلمية الرقمية المتجسدة في المعلومات المخزنة أو المنقولة بشكل رقمي وذلك وفق إجراءات خاصة تتفق وخصوصية الجريمة السيبرانية.[2]

---

[1] - إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة المصداقية، جامعة العربي التبسي – تبسة، المجلد 01، العدد 01، 2019، ص 114.

[2] - سمية بهلول، المرجع السابق، ص 310.

02- الوحدات التابعة للدرك الوطني:

تتمثل أساسا في:

أ) مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

أنشئ في سنة 2008 بالجزائر العاصمة، ويهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق و يوجد مقره ببئر مراد رايس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك.

ويهدف هذا المركز إلى مساعدة الأجهزة الأمنية الأخرى من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال إستغلال المعلومة من خلال التنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدا على الإستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها الوقاية و المكافحة.[1]

ب) المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلف بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة، كما يقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية و ضباط الشرطة القضائية والسلطات المؤهلة قانونيا خاصة أثناء معالجة القضايا المعقدة.

ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما فيما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الإختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.[2]

03- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:

تم إنشاء هذه المصلحة بتاريخ 06 نوفمبر 2015 على مستوى دائرة الإستعمال والتحضير لأركان الجيش الوطني الشعبي، وهذا في إطار الإستراتيجية المتبناة من أجل تحقيق نظام دفاع سيبراني متكامل وفعال. وهدفها تأمين حماية المنظومات والمنشآت الحيوية للبلاد ضد التهديدات والإرهاب الإلكتروني والجوسسة على أسرار الدولة و أي تهديد سيبراني، من خلال الرد السريع على الاختراقات والتشويش على أجهزة التجسس، وهي بذلك

[1] - إدريس عطية، المرجع السابق، ص 112-113.
[2] - المرجع نفسه، ص 113.

تعد طرفا فاعلا في العمليات العسكرية وتتمحور إستراتيجية الدفاع السيبراني للجيش حول محاور أساسية و تتمثل في الجوانب التالية:

- **الجانب الوظيفي:** من أجل ضمان فعالية و تناسق أعمال الدفاع السيبراني.

- **الجانب القانوني:** المكلف بتحيين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال عموما وتأمين منظومات الإعلام خصوصا.

- **الجانب البشري:** من خلال تكوين و كفاءة و جاهزية الموارد البشرية لأي هجوم سيبراني يهدد الأمن القومي الجزائري.[1]

- **الجانب التقني:** و يتعلق بمدى كفاءة الأجهزة و الوسائل المستعملة مع ضمان اليقظة للكشف و الرد على الهجمات السيبرانية.[2]

- **الجانب الوقائي و التحسيسي:** و ذلك بوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن استعمال تكنولوجيات الإعلام والاتصال في الإطار المهني أو الشخصي بطريقة مستمرة .

- **جانب البحث و التطوير:** تعد درجة معتبرة من الإستقلالية التكنولوجية ، باستعمال وسائل تقنية خاصة ومشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية عنصرا حاسما في إستراتيجية الدفاع السيبراني.

- **جانب التعاون:** تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل السماح لقوات الجيش الجزائري من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا.[3]

04- المركز الوطني للإشارة وأنظمة المعلومات والحرب الإلكترونية:

و هو أحد الأجهزة الأمنية التابع لوزارة الدفاع، و الذي يعنى بمكافحة الحروب و الجرائم السيبرانية التي تسعى لإختراق أمن الدولة، أنشأ سنة 2019 و هو تابع لدائرة الإشارة و أنظمة المعلومات و الحرب الإلكترونية حيث تسعى هذه الأخيرة للحفاظ على الدولة و أمنها السيبراني.[4]

---

[1] - عبد الله جعفري، التهديدات السيبرانية و تأثيرها على الأمن القومي الجزائري، المجلة الإفريقية للدراسات القانونية و السياسية، جامعة أحمد دراية أدرار، المجلد 06، العدد 02، 2022، ص 252.

[2] - المرجع نفسه، ص 253.

[3] - عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الباحث للدراسات و الأبحاث القانونية و القضائية، العدد 50، 2023، ص 37.

[4]- سلمة بورياح، السياسات العامة الجزائرية في محال السيبرانية الواقع والتحديات، دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، المجلد 15، العدد 01، 2023، ص 282.

05- المنظومة الوطنية لأمن الأنظمة المعلوماتية:

أقر المشرع الجزائري المنظومة الوطنية لأمن الأنظمة المعلوماتية كإستراتيجية جديدة لمكافحة الجرائم السيبرانية و ذلك بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، حيث تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني على كل من: المجلس الوطني لأمن الأنظمة المعلوماتية، و وكالة أمن الأنظمة المعلوماتية.[1]

أ- **المجلس الوطني لأمن أنظمة المعلوماتية:**

ويرأسه وزير الدفاع أو ممثله و يتولى المجلس في إطار إعداد الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتية:

- البت في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.
- دراسة مخطط عمل الوكالة و تقرير نشاطاتها والموافقة عليهما.
- دراسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.
- الموافقة على اتفاقات التعاون و الإعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني.
- الموافقة على تصنيف الأنظمة المعلوماتية.
- إقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، عند الحاجة، ويبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية. [2]

ب-**وكالة أمن الأنظمة المعلوماتية:**

تكلف الوكالة طبقا للمادة 18 من المرسوم الرئاسي رقم 20-05 على الخصوص بما يأتي:

- تحضير عناصر الإستراتيجية الوطنية في مجال أمن أنظمة المعلوماتية وعرضها على المجلس.
- تنسيق تنفيذ الإستراتيجية الوطنية لأمن أنظمة المعلوماتية المحددة من قبل المجلس.
- اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
- إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.
- السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن أنظمة المعلوماتية لإستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.
- متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.

[1] - دندن جمال الدين، الإستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، مجلة صوت القانون، جامعة الجيلالي بو نعامة، خميس مليانة، المجلد 07، العدد 02، 2020، ص 989-990

[2]- فتيحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي 20-05"، مجلة الحقوق و العلوم الإنسانية، جامعة زيان عاشور الجلفة، المجلد 13، العدد 03، 2020، ص 182.

– تقديم المشورة والمساعدة للإدارات والمؤسسات و الهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية.

– ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية.

– مرافقة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل المختصة في هذا المجال، في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية.

– إقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية، بعد الرأي المطابق للمجلس ....[1]

[1] - المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتـعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية الجزائرية العدد 04 الصادرة في 26 جانفي 2020.

الخلاصة:

أدى التحول الرقمي والإعتماد المتزايد على تكنولوجيا المعلومات والإتصالات والنمو المتواصل للجرائم السيبرانية، سواء من حيث التعقيد وإختلاف أساليبها و أشكالها و الإمكانات التخريبية لها، إلى زيادة غير مسبوقة في مخاطر الجرائم السيبرانية التي تواجه المجتمع والمنظمات الدولية، الأمر الذي أدى إلى تظافر الجهود الدولية و الإقليمية و الوطنية في مكافحة مختلف أشكال الجرائم السيبرانية.

وقد إنعكس الإهتمام العالمي بمكافحة الجرائم السيبرانية في مبادرات و جهود دولية و إقليمية مختلفة منها مبادرات و جهود الأمم المتحدة و الإتحاد الدولي للإتصالات في سياق القمم العالمية لمجتمع المعلومات و برامجها التنفيذية، كما تم تكثيف المبادرات الدولية و الإقليمية، والتي إنبثق منها العديد من المعاهدات و الإتفاقيات بما فيها الأوروبية و العربية و الإفريقية.

وفي إطار تعزيز التعاون الدولي لمجابهة الجرائم السيبرانية تم تفعيل آليات التعاون الشرطي المختلفة منها الدولية والإقليمية والتي تعد من أهم الآليات في مكافحة الجرائم السيبرانية والتي تعمل على محاربتها من خلال مجموعة من الإستراتيجيات الدفاعية وذلك بالتنسيق مع الأجهزة الشرطية المحلية للدول، وكذا تعاونها مع الهيئات الدولية ذات الصلة.

كما إنعكس الإهتمام الدولي والإقليمي بدوره في مكافحة الجرائم السيبرانية على المستوى الوطني، حيث تبنت الجزائر إستراتيجيات تشريعية و مؤسساتية في مواجهة تحديات الأمن السيبراني، إذ قامت بسن مجموعة من القوانين العامة و الخاصة و التي تهدف في مجملها إلى مكافحة الجرائم السيبرانية، بالإضافة إلى إرساء هيئات وطنية و مؤسسات أمنية تبذل هي الأخرى مجهودات جبارة في مكافحة تهديدات الفضاء السيبراني.

الخاتمة

الخـــــاتمة

في ختام هذه الدراسة يمكن القول أن تكنولوجيا الإتصالات والمعلومات وثقافة الإنترنت أصبحت من سمات العصر، فقد أسهمت في تغيير مفاهيم المكان و الزمان، حيث بات استخدام الأنظمة المعلوماتية من قبل الدول و الأفراد أمر لا غنى عنه في ظل تسريع إنجاز مختلف الأعمال في وقت قياسي، مما نجم عنه تحول العديد من المجتمعات إلى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها.

وفي الوقت الذي يتزايد فيه الإعتماد على الإنترنت ووسائل الإتصالات، فإن الجوانب الإيجابية التي يقدمها الفضاء السيبراني تأتي مصحوبة بمخاطر عديدة ناجمة عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي خلقت من أجله، الأمر الذي أثر على حقوق الأفراد وحرياتهم، حيث وفرت الأنظمة والتقنية الحديثة وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم، كما أضحى الفضاء السيبراني في ذاته محلاً للإعتداء عليه وإساءة إستخدامه.

واستناداً إلى ما سبق فإننا نخلص إلى ما يلي:

أولا/ نتائـــــج الدراســـــة.

1) الأمن السيبراني هو مجموعة من الأدوات و الوسائل و التقنيات التي يمكن إستخدامها لحماية الفضاء السيبراني من المخاطر المحدقة به ألا وهي الجرائم السيبرانية بمختلف أشكالها.
2) تطور الأمن السيبراني بالتوازي مع تطور أساليب و أشكال الجريمة السيبرانية، مما فتح سبل جديدة لتعزيز التدابير لمواجهة المخاطر و العمل على تدعيم البتية التحتية للدول و القطاع الخاص.
3) لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوما أن صناع القرار في العالم، أصبحوا يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية.
4) إن سوء الإستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلبا على سلامة الفضاء السيبراني، لاسيما على المعلومات الشخصية والبنى التحتية الأمنية الإستراتيجية.
5) للجرائم السيبرانية تأثير سلبي كبير على الحريات الفردية وحرمة الحياة الخاصة في حال إستخدام تكنولوجيا الإعلام والإتصال بشكل سلبي مخالف للقوانين و التنظيمات.
6) تسهم التكنولوجيا المتطورة في سرعة إنجاز الجريمة السيبرانية، الأمر الذي يضع الجهات الأمنية المختصة أمام تحدي إكتشاف الجريمة و هوية مرتكبها.
7) سعي المجتمع الدولي لمواجهة التحديات الجديدة الناجمة عن الجرائم السيبرانية بإعتبارها جرائم عابرة للقارات، و لتفادي الآثار الكارثية التي قد تسببها، و لتحقيق الأمن السيبراني الذي يحفظ السلامة الإلكترونية في الفضاء السيبراني من خلال مختلف الإتفاقيات الدولية و الإقليمية، و مساهمة مختلف الهيئات و المنظمات الدولية و الإقليمية إلى توحيد الرؤى بين الدول لمواجهة الجرائم السيبرانية، وخلق آليات تساعد في التحقيق و المتابعة القانونية للمجرم السيبراني.

8) حاول المشرع الجزائري جاهدا مسايرة التطور المستمر للجرائم السيبرانية وذلك بمكافحتها عن طريق سن مجموعة من القوانين العامة و الخاصة منها في سبيل حماية الحريات الفردية وحرمة الحياة الخاصة و حماية المجتمعات من التهديدات والإنتهاكات التي تحيط به في الفضاء السيبراني.
9) أمر المشرع الجزائري بتوفير منظومة متكاملة من الآليات المؤسساتية والفنية لضمان مواكبة ثورة المعلومات، والإحاطة بكل مستجدات الجرائم السيبرانية والعمل على الحد منها، فبالإضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف الجرائم السيبرانية.

ثانيـــا/ إقتراحـــات الدراســـــــة

1) نشر الوعي بمفهوم الأمن السيبراني و ذلك بالقيام بحملات توعوية بين مستخدمي شبكة الإنترنت لإتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان في الفضاء السيبراني، كما يجب توعيتهم بضرورة التحلي بثقافة التبليغ في الوقت اللازم لتتمكن الجهات المختصة من القيام بدورها في الوقت المناسب و التوصل إلى الجناة.
2) تنظيم الورشات و الندوات التكوينية التحسيسية حول أحدث تقنيات مكافحة الجرائم السيبرانية.
3) ضرورة إستحداث نصوص قانونية تحدد بشكل واضح ودقيق صور الجرائم السيبرانية وإيجاد العقوبات الملائمة لها التي من شأنها تحقيق الردع العام والخاص.
4) ضرورة وضع ميثاق دولي يلزم جميع الدول بالإنطواء تحته يهدف إلى حماية الحقوق و الحريات الفردية و حرمة الحياة الخاصة ضد مخاطر الإجرام السيبراني.
5) ضرورة تعزيز التعاون الدولي لمواجهة الجرائم السيبرانية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني في حال وقوعها وكيفية تسليم مجرمي المعلوماتية وغير ذلك من الأمور، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم السيبرانية.
6) تطوير آليات مكافحة الجرائم السيبرانية من خلال عقد المؤتمرات والندوات الدولية، وكذا الإتفاقيات الدولية التي سوف تساهم في توحيد إجراءات ملاحقة و توقيف و محاكمة المجرم السيبراني.
7) تكثيف الدورات والتكوينات المتخصصة و المستمرة في الجرائم السيبرانية للقضاة و لأعضاء النيابة العامة و كذا الضبطية القضائية حتى يكونوا على معرفة وإطلاع بكل ما هو جديد في مجال الأمن السيبراني و الجريمة السيبرانية.
8) جعل الأمن السيبراني من الإستراتيجيات الوطنية التي تعنى بالتنمية و التطوير.

قائمة

المصادر و المراجع

قائمة المصادر والمراجع:

أولا / الكتب:

1) الأمم المتحدة اللجنة الإقتصادية والإجتماعية لغربي آسيا، إرشادات الإسكوا للتشريعات السيبرانية، بيروت، 2012.
2) أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، سنة 2016.
3) أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والإقتصاد، الرياض، الطبعة الأولى، 2014.
4) بري محمود، السيبرنيطيقا (السيبرانية) علم القدرة على التواصل والتحكم والسيطرة، المركز الإسلامي للدراسة الإستراتيجية، بيروت، لبنان، الطبعة الأولى، 2019.
5) بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2014.
6) بيتر بيل سيل، الكون الرقمي: الثورة العالمية في الإتصالات، ترجمة ضياء وراد، هنداوي سي آي سي، 2017.
7) حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، دار الفكر والقانون للنشر والتوزيع، 2015.
8) حسنين شفيق، الاعلام الجديد والجرائم الإلكترونية، التسريبات، التجسس، الإرهاب الإلكتروني، دار فكر وفن للطباعة والنشر والتوزيع، 2014.
9) خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في جرائم المعلوماتية –دراسة مقارنة، مكتبة القانون والاقتصاد للنشر والتوزيع، الطبعة الأولى، 2014.
10) رفد عيادة الهاشمي، الإرهاب الإلكتروني، دار أمجد للنشر والتوزيع، عمان، 2019.
11) ساري محمد الخالد، اتجاهات في أمن المعلومات و أمنها، العبيكان للنشر و التوزيع، الرياض، الطبعة الأولى، 2018.
12) شادي عبد الوهاب منصور، حروب الجيل الخامس، العربي للنشر و التوزيع، الطبعة الأولى، 2019.
13) ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي: دراسة مقارنة، المركز العربي للنشر والتوزيع، القاهرة، الطبعة الأولى، 2017.
14) عادل عبد العزيز صالح الرشيد، قرائن الجريمة الإلكترونية و أثرها في الإثبات، دار كنوز إشبيليا للنشر و التوزيع، الرياض، المملكة العربية السعودية، الطبعة الاولى،2017.
15) عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون و الإقتصاد، الرياض، الطبعة الأولى، 2012.

16) عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمان، المحكمة الرقمية و الجريمة المعلوماتية، مكتبة القانون و الإقتصاد، الرياض، الطبعة الأولى، 2012.

17) علي جبار صالح الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، 2018.

18) علي زياد العلي، علي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، الطبعة الأولى، 2022.

19) غادة نصار، الإرهاب و الجريمة الالكترونية، العربي للنشر والتوزيع، القاهرة، 2017.

20) فارس محمد العمارات، إبراهيم الحمامصة، الأمن السيبراني–المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، الطبعة الاولى، 2022.

21) فارس محمد العمارات، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، الطبعة الاولى، 2023.

22) لورنس لسيج، الكود المنظّم للفضاء الإلكترونية، ترجمة :محمد سعد طنطاوي، مؤسسة هنداوي للتعليم والثقافة، القاهرة، طبعة 02، 2006.

23) مجمع البحوث و الدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الأمانة العامة، سلطنة عمان، 2016.

24) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية للصحافة و النشر، الطبعة الأولى، 2010.

25) محمد كمال، الإرهاب السيبراني، دار كليم للطباعة والنشر والتوزيع، القاهرة، مصر، الطبعة الأولى، 2022.

26) محمد محمود العمري، مدخل إلى الأمن السيبراني، دار زهران للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2020.

27) محمد مصطفى رفعت، الرأي العام في الواقع الافتراضي وقوة التعبئة الافتراضية، العربي للنشر والتوزيع، القاهرة، الطبعة الأولى، 2018.

28) محمود مدين، فن التحقيق والإثبات في الجرائم الالكترونية، المصرية للنشر والتوزيع، الطبعة الأولى، 2020.

29) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، الأمم المتحدة، نيويورك، 2013.

30) منى الأشقر جبور، البيانات الشخصية والقوانين العربية الهمّ الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت، لبنان، 2018.

31) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، لبنان، 2016.
32) ميرفت محمد حبايبة، مكافحة الجرائم الالكترونية – دراسة مقارنة – في التشريع الجزائري والفلسطيني، دار اليازوري العلمية للنشر و التوزيع، الأردن، 2022.
33) هشام بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز العربي للدراسات المستقبلية والإستراتيجية، مصر، 2012.
34) هيثم عبد الرحمان البقلي، الجرائم الإلكترونية الواقعة على العرض: بين الشريعة والقانون المقارن، دار العلوم للنشر والتوزيع، 2010.

ثانيا / المجلات العلمية والقانونية:

1) الإتحاد الدولي للإتصالات، شبكات البيانات والإتصالات بين الأنظمة المفتوحة و مسائل الأمن لمحة عامة عن الأمن السيبراني، التوصية رقم X.1205، سنة 2008.
2) إسراء شريف جيجان، الأمن السيبراني الصيني: دراسة في الدوافع والتحديات، مجلة قضايا سياسية، جامعة النهرين، العدد 65، 2022.
3) إسلام مصطفى جمعة مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) مجلة علمية محكمة، جامعة القاهرة، المجلد 12، العدد 3، 2022.
4) بارة سمير، الأمن السيبراني (Cyber Security) في الجزائر: السياسات و المؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، المجلد 02، العدد 02، 2017.
5) بن جدو بن علية، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، المجلد 07، العدد 02، 2022.
6) بن دريس حليمة، حماية الأطفال ضحايا الجرائم الإلكترونية، مجلة المفكر للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، العدد 06، 2019.
7) بهلول سمية، الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها، مجلة العلوم القانونية والإجتماعية، جامعة الجلفة زيان عاشور، المجلد 06، العدد 04، 2021.
8) بورياح سلمة، السياسات العامة الجزائرية في محال السيبرانية الواقع والتحديات، دفاتر السياسة و القانون، جامعة قاصدي مرباح ورقلة، المجلد 15، العدد 01، 2023.
9) بوعزة نضيرة، المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث و الدراسات، المركز الجامعي عبد الحفيظ بوصوف ميلة، المجلد 07، العدد 01، 2021.

10) بيدي أمال، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، جامعة تيارت، المجلد 08، العدد 01، 2022.

11) تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، المجلد 08، العدد 33 – 34، 2020.

12) جعفري عبد الله، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية أدرار، المجلد 06، العدد 02، 2022.

13) جيلالي دلالي، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، 2021.

14) حاجي نعيمة، الجريمة السيبرانية والجهود الدولية لمكافحتها، مجلة النبراس للدراسات القانونية، المجلد 06، جامعة العربي التبسي–تبسة، العدد 01، 2021.

15) حازم محمد خليل، إستغلال الفضاء السيبراني في الحروب غسر التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الإقتصادية والعلوم السياسية بجامعة الإسكندرية، المجلد 08، العدد 25، 2023.

16) حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي 20–05"، مجلة الحقوق و العلوم الإنسانية، جامعة زيان عاشور الجلفة، المجلد 13، العدد 03، 2020، ص 182

17) حمري نجود، حمري نوال، واقع التجارة الالكترونية في الجزائر وفق مقتضيات قانون رقم 18–05 (قانون التجارة الالكترونية) ، مجلة البحوث القانونية والاقتصادية، المركز الجامعي بآفلو، المجلد 04، العدد 01، 2021.

18) خالد ظاهر عبد الله جابر السهيل المطري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية و القانونية، جامعة الأزهر، المجلد 38، العدد38، 2022.

19) خلود عاصم ومحمد ابراهيم، دور تكنولوجيا المعلومات والاتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية الجامعة، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013.

20) خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكولاي لوزينسكي، الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، الأمم المتحدة، جنيف، 2021.

21) دلالي جيلالي، بلبشير يعقوب، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، مجلة كلية القانون الكويتية العالمية، المجلد 10، العدد 01، 2021.

22) دندن جمال الدين، الإستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، مجلة صوت القانون، جامعة الجيلالي بو نعامة، خميس مليانة، المجلد 07، العدد 02، 2020.

23) رانا مصباح عبد المحسن عبد الرازق، آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية"، المجلة القانونية، جامعة القاهرة، المجلد 15، العدد 05، 2023.

24) زناتي محمد السعيد، جواج يمينة، أثر الجرائم السيبرانية عمى الحريات الفردية (الجزائر نموذجا)، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية أدرار، المجلد 06، العدد 01، 2022.

25) زياد بن محمد عادي العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث أشكالها، خصاصها، أركانها و الدافع من إرتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، عمان، الأردن، المجلد 03، العدد 01، 2020.

26) ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الإجتماعية، الجزائر، المجلد 03، العدد 1، 2022.

27) سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني دراسة في ضوء احكام القانون الدولي العام، مجلة لارك للفلسفة و اللسانيات و العلوم الاجتماعية، المجلد 03، العدد 46، 2022،

28) سامية بساعد، حماية البيانات الشخصية للمستهلك من مخاطر الدفع الإلكتروني، مجلة الحقوق والعلوم الإنسانية، جامعة الشهيد زيان عاشور الجلفة، المجلد 15، العدد 01، 2022.

29) سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، المجلد ب، العدد 52، 2019.

30) سهام حسن علي الشمري، تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية، جامعة بغداد، العدد 83، 2020.

31) شرف الدين وردة، بلجراف سامية، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، جامعة يحي فارس المدية، المجلد 01، العدد 03، 2017.

32) شرون حسينة، قفاف فاطمة، الدور الحمائي للهيئة الوطنية لحماية و ترقية الطفولة، حوليات جامعة الجزائر 1، الجزء الثاني، العدد 32، 2018.

33) شريهان ممدوح حسن، الجرائم المعلوماتية و سبل مواجهتها على المستويين الوطني و الدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية و التربوية، عمان الأردن، العدد 21، 2020.

34) شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 01، 2020.

35) شيخي عائشة، بوزيان عياشي، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأشكالها الإقتصادية وآليات مكافحتها، مجلة الدراسات الحقوقية، جامعة الدكتور الطاهر مولاي سعيدة، العدد الرابع، 2015.

36) صفرة بشيرة، حماية المصنفات الرقمية في التشريع الجزائري، مجلة الحقوق و العلوم الإنسانية، جامعة الجلفة، المجلد 01، العدد 29، 2016.

37) صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، جامعة النهرين، المجلد 12، العدد 62، 2020.

38) عادل عبد الصادق، الفضاء الالكتروني والرأي العام: تغير المجتمع والأدوات والتأثير، قضايا استراتيجية، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2009.

39) عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية، جامعة الأزهر، المجلد 16، العدد 1، 2014.

40) عبد الحميد عائشة، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الباحث للدراسات والأبحاث القانونية و القضائية، العدد 50، 2023.

41) عبيشات أمينة، الجرائم الإلكترونية بين المواثيق الدولية و التشريعات الوطنية، المجلة الجزائرية للحقوق و العلوم السياسية، المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت، المجلد 06، العدد 01، 2021.

42) عطية إدريس، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة المصداقية، جامعة العربي التبسي – تبسة، المجلد 01، العدد 01، 2019.

43) عقل يوسف مقابلة، مواجهة الإرهاب السيبراني في القانون الجزائي الأردني والمعاهدات الدولية، المجلة الدولية للدراسات القانونية والفقهية المقارنة، الأردن، المجلد 01، العدد 03، 2020.

44) علي محمد منيف الرفيعي، تحديات الأمن في الفضاء السيبراني الأمريكي، مجلة دراسات دولية، جامعة بغداد، المجلد 20، العدد 85، 2021.

45) عميش وهيبة، دور الهيئات الوطنية لحماية المصنفات الرقمية في القانون الجزائري، القانونية الدراسات القانونية، جامعة يحي فارس المدية، المجلد 08، العدد 01، 2022.

46) العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي علي كافي تندوف، العدد 05، 2018.

47) عيساني طـه، عبد الله فوزية، المصنفات الرقمية المشمولة بالحماية بموجب قوانين الملكية الفكرية في الاتفاقيات الدولية والقانون الجزائري، دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، المجلد 13، العدد 10، 2021.

48) غسان قاسم داود، تحليل مكونات البنية التحتية لتكنولوجيا المعلومة دراسة استطلاعية في بيئة عمل عراقية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013.

49) فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق و الحريات، جامعة محمد خيضر بسكرة، المجلد 03، العدد 02، 2015.

50) فرحات علاء الدين، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي و العشرين، مجلة العلوم القانونية و السياسية، جامعة الشهيد حمه لخضر الوادي، المجلد 10، العدد 03، 2019.
51) قطاف سليمان، بوقرين عبد الحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 06، العدد 01، 2022.

52) قطاف سليمان، بوقرين عبد الحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي بآفلو، المجلد 05، العدد 02، 2022.
53) كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية لقانون الأعمال، جامعة محمد بوضياف المسيلة، المجلد 01، العدد 02، 2020.
54) كحيلة سارة، أمن وحامية الوثائق الإلكترونية من خلال المعايير الدولية والنصوص التشريعية، .Aleph Langues, médias et sociétés ، جامعة الجزائر 2، المجلد 08، العدد 03، 2021.
55) لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، المجلد 08، العدد 33 – 34، 2020.

56) لزعر عزيز، زياني رشيد، آلية الاتحاد الإفريقي للتعاون الشرطي (الأفريبول) و دورها في مكافحة الجريمة الإلكترونية، مجلة متون، جامعة الدكتور مولاي الطاهر سعيدة، المجلد 14، العدد 03، 2021.
57) لوكال مريم، قراءة في إتفاقية الإتحاد الإفريقي حول الأمن السيبراني و حماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية و الإقتصادية، المركز الجامعي سي الحواس بريكة، المجلد 04، العدد 03، 2021.
58) ليتيم نادية، حقوق الطفل بالإتحاد الأوروبي دراسة تحليلية في آليات الحماية القانونية والإستراتيجية، مجلة الحقوق والعلوم الإنسانية، جامعة الشهيد زيان عاشور الجلفة، المجلد 14، العدد 03، 2021.
59) محمود علي عبد الرحمان، أسامة فاروق مخيمر، الفضاء الالكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، جامعة بني سويف، مصر، المجلد 16، العدد 15، 2022.

60) مسيكة محمد، الفضاء السيبراني وتحديات الأمن القومي للدول، جملة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، المجلد 07، العدد 04، 2022.
61) مشوش مراد، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 12، العدد 02، 2019.
62) منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، مصر، العدد 111، 2020.

63) مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المركز الجامعي المقاوم الشيخ آمود بن مختار إليزي، المجلد 06، العدد 02، 2021.
64) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، الجلد 8، العدد 2، 2018.
65) ياكر الطاهر، مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد 04، العدد 04، 2022.

ثالثا/ القوانين و المراسيم:

1) دستور الجزائر لسنة 2020، المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية العدد 82 الصادرة بتاريخ 30 ديسمبر 2020.
2) قانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 71 الصادر 10 نوفمبر 2004.
3) قانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 06-156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 الصادر بتاريخ 10 نوفمبر 2004.
4) قانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11 المؤرخ في 02 يوليو 1983 المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية عدد 04 الصادرة بتاريخ 27 يناير 2008.
5) قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، الصادرة في 25 شعبان 1430 الموافق لـ 16 غشت 2009.
6) قانون رقم 14-01 المؤرخ في 04 فيفري 2014، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 07 الصادر بتاريخ 16 فيفري 2014.
7) قانون رقم 15-12 مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015، يتعلق بحماية الطفل، الجريدة الرسمية الجزائرية عدد 39 الصادر بتاريخ 19 يوليو 2015.
8) قانون رقم 16-02 المؤرخ في 19 جوان 2016، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات، الجريدة الرسمية عدد 37 الصادر بتاريخ 22 جوان 2016.
9) قانون رقم 18-04 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية عدد 27، الصادرة بتاريخ 13 ماي 2018.
10) قانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد 28، الصادرة بتاريخ 16 ماي 2018.

11) قانون رقم 18-07 المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 الصدرة بتاريخ 10 جوان 2018.
12) قانون رقم 23-04 المؤرخ في 07 ماي 2023، المتعلق بالوقاية من الإتجار بالبشر ومكافحته، الجريدة الرسمية عدد 32، الصادرة بتاريخ 09 ماي 2023.
13) المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية الجزائرية العدد 04 الصادرة في 26 جانفي 2020.
14) المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 40 الصادرة بتاريخ 18 يوليو 2020.
15) مرسوم تنفيذي رقم 05-356 المؤرخ في 21 سبتمبر 2005، المتضمن القانون الأساسي للديوان الوطني لحقوق المؤلف و الحقوق المجاورة و تنظيمه و سيره، الجريدة الرسمية الجزائرية عدد 65 الصادر بتاريخ 21 سبتمبر 2005.
16) مرسوم تنفيذي رقم 16-334 المؤرخ في 19 ديسمبر 2016 يحدد شروط و كيفيات تنظيم و سير الهيئة الوطنية لحماية و ترقية الطفولة، الجريدة الرسمية عدد 75 الصادرة بتاريخ 21 ديسمبر 2016.
17) الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى سنة 1424 الموافق 19 يوليو عام 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية العدد 44 الصادر بتاريخ 23 يوليو 2003.
18) أمر رقم 21-11 المؤرخ في 25 أوت 2021، المتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 65 الصادرة بتاريخ 26 أوت 2021.

رابعا/ قوانين أجنبية:

1) قانون رقم 20-05 المؤرخ بتطوان في 4 ذي الحجة 1441 (25 يوليو 2020)، المتعلق بالأمن السيبراني، الجريدة الرسمية للمملكة المغربية، عدد 6904، الصادر في 9 ذي الحجة 1441 (30 يوليو 2020).
2) قانون رقم 16 لسنة 2019، الامن السيبراني، الجريدة الرسمية للملكة الاردنية الهاشمية، عدد 5595، الصادرة في 16 سبتمبر 2019.

خامسا/ قرارات:

1) الجمعية العامة للأمم المتحدة، قرارات الدورة 74، قرار رقم (247/74) المؤرخ في 27 ديسمبر 2019، البند رقم 107.

سادسا/ المواقع الإلكترونية:

1) فارس قوة، الأمن السيبراني ، Cyber Security، الموسوعة السياسية، رابط الموقع:
https://political-encyclopedia.org/dictionary/الأمن%20السيبراني

2) إيهاب عبد الحميد خليفة، الفضاء الإلكتروني وتهديد ات الأمن القومي المصري ، المركز العربي لأبحاث الفضاء الإلكتروني، 2013 ، على الرابط:
http://www.accronline.com/print_article.aspx?id=15383

3) المركز الأوروبي للجرائم الإلكترونية EC3 (التحديث بتاريخ 01 مارس 2022) ، تم الإطلاع عليه بتاريخ :2023/04/17 ، رابط الموقع:
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

الفهرس

الفصـــل الثانـــــي

آليات مكافحة الجرائم السيبرانية

الملخص:

أدى التحول الرقمي و الإعتماد المتزايد على تكنولوجيا المعلومات و الإتصال الذي يشهده العالم إلى بروز مفاهيم جديدة منها الفضاء السيبراني، و الذي تتم فيه جميع التفاعلات الرقمية.

حيث شهد الفضاء السيبراني تزايد عدد الهجمات السيبرانية بشكل كبير و مستمر، نظرا لتعدد و إختلاف أشكال الجرائم السيبرانية، مما إستدعى ضرورة و جود ضمانات أمنية ضمن تحمي الفضاء السيبراني من الجرائم السيبرانية، تبورت بشكل أساسي في ظهور الامن السيبراني الذي أصبح يشكل جزءا أساسيا لمكافحة الجرائم السيبرانية على المستوى الوطني و الدولي.

الكلمات المفتاحية: الأمن السيبراني، الفضاء السيبراني، الجرائم السيبرانية، آليات مكافحة الجرائم السيبرانية.

Abstract :

The digital transformation and the increasing dependence on information and communication technologies witnessed by the world have led to the emergence of new concepts, including cyberspace, which all digital interactions take place in.

The cyberspace has witnessed a significant and continuous increase in the number of cyber-attacks, due to the multiplicity and variety of forms of cybercrimes, which necessitated the necessity and existence of security guarantees within the protection of cyberspace from cybercrimes, mainly manifested in the emergence of cyber security, which has become an essential part of the fight against cybercrimes at the national and international levels.

Keywords: cyber security, cyber space, cyber-crimes, Mechanisms for combating cybercrime.